Hewlett Packard Enterprise

HPE FlexNetwork 5510 HI Switch Series

Layer 2—LAN Switching Configuration Guide

Part number: 5200-0075b
Software version: Release 11xx
Document version: 6W102-20171020

© Copyright 2015, 2017 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

Configuring Ethernet interfaces ····· 1
Configuring a management Ethernet interface ····· 1
Ethernet interface naming conventions ····· 1
Configuring common Ethernet interface settings ····· 1
Configuring a combo interface (only applicable to HPE 5510 24G SFP 4SFP+ HI 1-slot Switch (JH149A) switches) ····· 2
Splitting a 40-GE interface and combining 10-GE breakout interfaces ····· 2
Configuring basic settings of an Ethernet interface ····· 3
Configuring the link mode of an Ethernet interface ····· 4
Configuring jumbo frame support ····· 4
Configuring physical state change suppression on an Ethernet interface ····· 5
Performing a loopback test on an Ethernet interface ····· 6
Configuring generic flow control on an Ethernet interface ····· 6
Enabling energy saving features on an Ethernet interface ····· 7
Setting the statistics polling interval ····· 8
Configuring the interface card operating mode ····· 8
Enabling automatic negotiation for speed downgrading ····· 9
Configuring a Layer 2 Ethernet interface ····· 9
Configuring storm suppression ····· 9
Configuring storm control on an Ethernet interface ····· 10
Forcibly bringing up a fiber port ····· 12
Setting the MDIX mode of an Ethernet interface ····· 13
Testing the cable connection of an Ethernet interface ····· 14
Enabling bridging on an Ethernet interface ····· 14
Configuring a Layer 3 Ethernet interface ····· 14
Setting the MTU for an Ethernet interface ····· 14
Displaying and maintaining an Ethernet interface ····· 15
Configuring loopback, null, and inloopback interfaces ····· 16
Configuring a loopback interface ····· 16
Configuring a null interface ····· 16
Configuring an inloopback interface ····· 17
Displaying and maintaining loopback, null, and inloopback interfaces ····· 17
Bulk configuring interfaces ····· 18
Configuration restrictions and guidelines ····· 18
Configuration procedure ····· 18
Displaying and maintaining bulk interface configuration ····· 19
Configuring the MAC address table ····· 20
Overview ····· 20
How a MAC address entry is created ····· 20
Types of MAC address entries ····· 20
MAC address table configuration task list ····· 21
Configuring MAC address entries ····· 22
Configuration guidelines ····· 22
Adding or modifying a static or dynamic MAC address entry globally ····· 22
Adding or modifying a static or dynamic MAC address entry on an interface ····· 22
Adding or modifying a blackhole MAC address entry ····· 23
Adding or modifying a multiport unicast MAC address entry ····· 23
Disabling MAC address learning ····· 24
Disabling global MAC address learning ····· 24
Disabling MAC address learning on an interface ····· 25
Disabling MAC address learning on a VLAN ····· 25
Configuring the aging timer for dynamic MAC address entries ····· 25
Configuring the MAC learning limit on an interface ····· 26
Configuring the device to forward unknown frames after the MAC learning limit on an interface is reached ····· 26

Assigning MAC learning priority to an interface 27
Enabling MAC address synchronization 28
Enable MAC address move notifications 29
Enabling ARP fast update for MAC address moves 30
Enabling SNMP notifications for the MAC address table 31
Displaying and maintaining the MAC address table 31
MAC address table configuration example 32
Network requirements 32
Configuration procedure 32
Verifying the configuration 33
Configuring MAC Information 34
Enabling MAC Information 34
Configuring the MAC Information mode 34
Configuring the MAC change notification interval 35
Configuring the MAC Information queue length 35
MAC Information configuration example 35
Network requirements 35
Configuration restrictions and guidelines 36
Configuration procedure 36
Configuring Ethernet link aggregation 38
Basic concepts 38
Aggregation group, member port, and aggregate interface 38
Aggregation states of member ports in an aggregation group 38
Operational key 39
Configuration types 39
Link aggregation modes 40
Aggregating links in static mode 40
Choosing a reference port 40
Setting the aggregation state of each member port 40
Aggregating links in dynamic mode 41
LACP 41
How dynamic link aggregation works 42
Edge aggregate interface 45
Load sharing modes for link aggregation groups 45
Ethernet link aggregation configuration task list 45
Configuring an aggregation group 46
Configuration restrictions and guidelines 46
Configuring a static aggregation group 46
Configuring a dynamic aggregation group 47
Configuring an aggregate interface 49
Configuring the description of an aggregate interface 49
Specifying ignored VLANs for a Layer 2 aggregate interface 50
Setting the MTU for a Layer 3 aggregate interface 50
Setting the minimum and maximum numbers of Selected ports for an aggregation group 50
Setting the expected bandwidth for an aggregate interface 51
Configuring an edge aggregate interface 51
Enabling BFD for an aggregation group 52
Shutting down an aggregate interface 53
Restoring the default settings for an aggregate interface 53
Configuring load sharing for link aggregation groups 54
Setting load sharing modes for link aggregation groups 54
Enabling local-first load sharing for link aggregation 55
Configuring per-flow load sharing algorithm settings for Ethernet link aggregation 55
Enabling link-aggregation traffic redirection 56
Configuration restrictions and guidelines 56
Configuration procedure 57
Specifying link aggregation management VLANs and management port 57
Displaying and maintaining Ethernet link aggregation 58
Ethernet link aggregation configuration examples 58
Layer 2 static aggregation configuration example 58

Layer 2 dynamic aggregation configuration example 60
Layer 2 aggregation load sharing configuration example 62
Layer 2 edge aggregate interface configuration example 64
Layer 3 static aggregation configuration example 66
Layer 3 dynamic aggregation configuration example 67
Layer 3 edge aggregate interface configuration example 68
Configuring port isolation 70
Assigning a port to an isolation group 70
Displaying and maintaining port isolation 70
Port isolation configuration example 71
Network requirements 71
Configuration procedure 71
Verifying the configuration 71
Configuring spanning tree protocols 73
STP 73
STP protocol packets 73
Basic concepts in STP 73
Calculation process of the STP algorithm 74
RSTP 80
PVST 80
MSTP 80
MSTP features 81
MSTP basic concepts 81
How MSTP works 85
MSTP implementation on devices 85
Protocols and standards 86
Spanning tree configuration task lists 86
STP configuration task list 87
RSTP configuration task list 87
PVST configuration task list 88
MSTP configuration task list 88
Setting the spanning tree mode 89
Configuring an MST region 90
Configuring the root bridge or a secondary root bridge 91
Configuring the current device as the root bridge of a specific spanning tree 91
Configuring the current device as a secondary root bridge of a specific spanning tree 91
Configuring the device priority 92
Configuring the maximum hops of an MST region 92
Configuring the network diameter of a switched network 93
Configuring spanning tree timers 93
Configuration restrictions and guidelines 94
Configuration procedure 94
Configuring the timeout factor 95
Configuring the BPDU transmission rate 95
Configuring edge ports 95
Configuration restrictions and guidelines 96
Configuration procedure 96
Configuring path costs of ports 96
Specifying a standard for the device to use when it calculates the default path cost 96
Configuring path costs of ports 98
Configuration example 99
Configuring the port priority 99
Configuring the port link type 100
Configuration restrictions and guidelines 100
Configuration procedure 100
Configuring the mode a port uses to recognize and send MSTP packets 100
Enabling outputting port state transition information 101
Enabling the spanning tree feature 101
Enabling the spanning tree feature in STP/RSTP/MSTP mode 102
Enabling the spanning tree feature in PVST mode 102

Performing mCheck 102
Configuration restrictions and guidelines 103
Configuration procedure 103
Configuring Digest Snooping 103
Configuration restrictions and guidelines 104
Configuration procedure 104
Digest Snooping configuration example 104
Configuring No Agreement Check 105
Configuration prerequisites 106
Configuration procedure 107
No Agreement Check configuration example 107
Configuring TC Snooping 107
Configuration restrictions and guidelines 108
Configuration procedure 108
Configuring protection functions 108
Enabling BPDU guard 109
Enabling root guard 109
Enabling loop guard 110
Configuring port role restriction 110
Configuring TC-BPDU transmission restriction 111
Enabling TC-BPDU guard 111
Enabling BPDU drop 112
About dispute guard 112
Displaying and maintaining the spanning tree 113
Spanning tree configuration example 114
MSTP configuration example 114
PVST configuration example 117
Configuring loop detection 121
Overview 121
Loop detection mechanism 121
Loop detection interval 122
Loop protection actions 122
Port status auto recovery 122
Loop detection configuration task list 123
Enabling loop detection 123
Enabling loop detection globally 123
Enabling loop detection on a port 123
Configuring the loop protection action 124
Configuring the global loop protection action 124
Configuring the loop protection action on a Layer 2 Ethernet interface 124
Configuring the loop protection action on a Layer 2 aggregate interface 124
Setting the loop detection interval 124
Displaying and maintaining loop detection 125
Loop detection configuration example 125
Network requirements 125
Configuration procedure 125
Verifying the configuration 126
Configuring VLANs 128
Overview 128
VLAN frame encapsulation 128
Protocols and standards 129
Configuring basic VLAN settings 129
Configuring basic settings of a VLAN interface 130
Configuring port-based VLANs 131
Introduction 131
Assigning an access port to a VLAN 132
Assigning a trunk port to a VLAN 133
Assigning a hybrid port to a VLAN 133
Configuring MAC-based VLANs 134
Introduction 134

Configuration restrictions and guidelines 137
Configuring static MAC-based VLAN assignment 137
Configuring dynamic MAC-based VLAN assignment 138
Configuring server-assigned MAC-based VLAN 138
Configuring IP subnet-based VLANs 139
Configuring protocol-based VLANs 140
Configuring a VLAN group 141
Displaying and maintaining VLANs 142
VLAN configuration examples 142
Port-based VLAN configuration example 142
MAC-based VLAN configuration example 144
IP subnet-based VLAN configuration example 146
Protocol-based VLAN configuration example 147
Configuring super VLANs 151
Super VLAN configuration task list 151
Creating a sub-VLAN 151
Configuring a super VLAN 151
Configuring a super VLAN interface 152
Displaying and maintaining super VLANs 152
Super VLAN configuration example 153
Network requirements 153
Configuration procedure 153
Verifying the configuration 154
Configuring the private VLAN 156
Configuration task list 156
Configuration restrictions and guidelines 157
Configuration procedure 157
Displaying and maintaining the private VLAN 159
Private VLAN configuration examples 159
Promiscuous port configuration example 159
Trunk promiscuous port configuration example 162
Trunk promiscuous and trunk secondary port configuration example 165
Secondary VLAN Layer 3 communication configuration example 170
Configuring voice VLANs 173
Overview 173
Methods of identifying IP phones 173
Identifying IP phones through OUI addresses 173
Automatically identifying IP phones through LLDP 174
Advertising the voice VLAN information to IP phones 174
IP phone access methods 175
Connecting the host and the IP phone in series 175
Connecting the IP phone to the device 175
Configuring a voice VLAN on a port 175
Voice VLAN assignment modes 175
Security mode and normal mode of voice VLANs 177
Configuration prerequisites 178
Configuring the QoS priority settings for voice traffic 178
Configuring a port to operate in automatic voice VLAN assignment mode 179
Configuring a port to operate in manual voice VLAN assignment mode 180
Enabling LLDP for automatic IP phone discovery 181
Configuration prerequisites 181
Configuration restrictions and guidelines 181
Configuration procedure 181
Configuring LLDP or CDP to advertise a voice VLAN 181
Dynamically advertising an authorization VLAN through LLDP or CDP 182
Displaying and maintaining voice VLANs 183
Voice VLAN configuration examples 183
Automatic voice VLAN assignment mode configuration example 183
Manual voice VLAN assignment mode configuration example 185

Configuring MVRP 187
MRP 187
MRP implementation 187
MRP messages 187
MRP timers 189
MVRP registration modes 190
Protocols and standards 190
MVRP configuration task list 190
Configuration restrictions and guidelines 190
Configuration prerequisites 191
Enabling MVRP 191
Setting an MVRP registration mode 192
Setting MRP timers 192
Enabling GVRP compatibility 193
Displaying and maintaining MVRP 193
MVRP configuration example 193
Network requirements 193
Configuration procedure 194
Verifying the configuration 197
Configuring QinQ 204
Overview 204
How QinQ works 204
QinQ implementations 205
Protocols and standards 205
Restrictions and guidelines 206
Enabling QinQ 206
Configuring transparent transmission for VLANs 206
Configuring the TPID in VLAN tags 207
Configuring the CVLAN TPID 208
Configuring the SVLAN TPID 208
Setting the 802.1p priority in SVLAN tags 208
Displaying and maintaining QinQ 209
QinQ configuration examples 210
Basic QinQ configuration example 210
VLAN transparent transmission configuration example 212
Configuring VLAN mapping 214
Overview 214
Application scenario of one-to-one and many-to-one VLAN mapping 214
Application scenario of one-to-two and two-to-two VLAN mapping 216
VLAN mapping implementations 216
General configuration restrictions and guidelines 219
VLAN mapping configuration task list 219
Configuring one-to-one VLAN mapping 220
Configuring many-to-one VLAN mapping 220
Configuring many-to-one VLAN mapping in a network with dynamic IP address assignment 221
Configuring many-to-one VLAN mapping in a network with static IP address assignment 223
Configuring one-to-two VLAN mapping 225
Configuring two-to-two VLAN mapping 225
Displaying and maintaining VLAN mapping 226
VLAN mapping configuration examples 226
One-to-one and many-to-one VLAN mapping configuration example 226
One-to-two and two-to-two VLAN mapping configuration example 231
Configuring LLDP 234
Overview 234
Basic concepts 234
Working mechanism 239
Protocols and standards 240
LLDP configuration task list 240

Performing basic LLDP configurations 240
Enabling LLDP 240
Configuring the LLDP bridge mode 241
Setting the LLDP operating mode 242
Setting the LLDP reinitialization delay 242
Enabling LLDP polling 242
Configuring the advertisable TLVs 243
Configuring the management address and its encoding format 245
Setting other LLDP parameters 246
Setting an encapsulation format for LLDP frames 246
Configuring CDP compatibility 247
Configuration prerequisites 248
Configuration procedure 248
Configuring LLDP trapping and LLDP-MED trapping 248
Displaying and maintaining LLDP 249
LLDP configuration examples 250
Basic LLDP configuration example 250
CDP-compatible LLDP configuration example 254
Configuring service loopback groups 256
Configuration procedure 256
Displaying and maintaining service loopback groups 256
Service loopback group configuration example 257
Network requirements 257
Configuration procedure 257
Document conventions and icons 258
Conventions 258
Network topology icons 259
Support and other resources 260
Accessing Hewlett Packard Enterprise Support 260
Accessing updates 260
Websites 261
Customer self repair 261
Remote support 261
Documentation feedback 261
Index 263

Configuring Ethernet interfaces

The switch series supports Ethernet interfaces, management Ethernet interfaces, Console interfaces, and USB interfaces. For the interface types and the number of interfaces supported by a switch model, see the installation guide.

This document describes how to configure management Ethernet interfaces and Ethernet interfaces.

Configuring a management Ethernet interface

A management interface uses an RJ-45 connector. You can connect the interface to a PC for software loading and system debugging, or connect it to a remote NMS for remote system management.

Support for management Ethernet interfaces depends on the device model. For more information, see the installation guide.

To configure a management Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter management Ethernet interface view.	**interface M-GigabitEthernet** *interface-number*	N/A
3. (Optional.) Set the interface description.	**description** *text*	The default setting is **M-GigabitEthernet0/0/0 Interface**.
4. (Optional.) Shut down the interface.	**shutdown**	By default, the management Ethernet interface is up.

Ethernet interface naming conventions

The Ethernet interfaces are named in the format of *interface type A/B/C*. The letters that follow the interface type represent the following elements:

- **A**—IRF member ID. If the switch is not in an IRF fabric, A is 1 by default.
- **B**—Card slot number. **0** indicates the interface is a fixed interface of the switch. **1** indicates the interface is on expansion interface-card 1. **2** indicates the interface is on expansion interface-card 2.
- **C**—Port index.

A 10-GE breakout interface split from a 40-GE interface is named in the format of interface type A/B/C:D. A/B/C is the interface number of the 40-GE interface and D is the number of the 10-GE interface, which is in the range of 1 to 4. For information about splitting a 40-GE interface, see "Splitting a 40-GE interface and combining 10-GE breakout interfaces."

Configuring common Ethernet interface settings

This section describes the settings common to Layer 2 and Layer 3 Ethernet interfaces. You can set an Ethernet interface as a Layer 3 interface by using the **port link-mode route** command. For more information, see "Configuring the link mode of an Ethernet interface." For more information about the settings specific to Layer 2 and Layer 3 Ethernet interfaces, see "Configuring a Layer 2 Ethernet interface" and "Configuring a Layer 3 Ethernet interface."

Configuring a combo interface (only applicable to HPE 5510 24G SFP 4SFP+ HI 1-slot Switch (JH149A) switches)

A combo interface is a logical interface that physically contains one fiber combo port and one copper combo port. The two ports share one forwarding channel and one interface view. As a result, they cannot work simultaneously. When you activate one port, the other port is automatically disabled. In the interface view, you can activate the fiber or copper combo port, and configure other port attributes such as the interface rate and duplex mode.

For more information about the number of combo interfaces, see the installation guide.

Configuration prerequisites

Use the **display interface** command to determine which port (fiber or copper) of each combo interface is active:

- If the copper port is active, the output includes "Media type is twisted pair."
- If the fiber port is active, the output does not include this information.

Also, you can use the **display this** command in the view of each combo interface to display the combo interface configuration:

- If the fiber port is active, the **combo enable fiber** command exists in the output.
- If the copper port is active, the **combo enable fiber** command does not exist in the output.

Changing the active port of a combo interface

Step	Command	Remarks
5. Enter system view.	**system-view**	N/A
6. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
7. Activate the copper combo port or fiber combo port.	**combo enable** { **copper** | **fiber** }	By default, the copper combo port is active.

Splitting a 40-GE interface and combining 10-GE breakout interfaces

Splitting a 40-GE QSFP+ interface into four 10-GE breakout interfaces

You can use a 40-GE QSFP+ interface as a single interface. To improve port density, reduce costs, and improve network flexibility, you can also split a 40-GE QSFP+ interface into four 10-GE breakout interfaces.

After the **using tengige** command is successfully configured, reboot your device as needed. For more information, see *Layer 2—LAN Switching Command Reference*.

A 40-GE interface split into four 10-GE breakout interfaces must use a dedicated 1-to-4 cable. For more information about the cable, see the installation guides.

To split a 40-GE interface into four 10-GE breakout interfaces:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter 40-GE interface view.	**interface** *interface-type interface-number*	N/A

Step	Command	Remarks
3. Split the 40-GE interface into four 10-GE breakout interfaces.	**using tengige**	By default, a 40-GE interface is not split and operates as a single interface. The 10-GE breakout interfaces split from a 40-GE interface support the same configuration and attributes as common 10-GE interfaces, except that they are numbered in a different way.

Combining four 10-GE breakout interfaces into a 40-GE interface

If you need higher bandwidth, you can combine the four 10-GE breakout interfaces into a 40-GE interface.

After the **using fortygige** command is successfully configured, reboot your device as needed. For more information, see *Layer 2—LAN Switching Command Reference*.

After you combine the four 10-GE breakout interfaces, replace the dedicated 1-to-4 cable with a dedicated 1-to-1 cable or a 40-GE transceiver module. For more information about the cable or transceiver module, see the installation guides.

To combine four 10-GE breakout interfaces into a 40-GE interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter the view of any 10-GE breakout interface split from a 40-GE interface.	**interface** *interface-type interface-number*	N/A
3. Combine the four 10-GE breakout interfaces into a 40-GE interface.	**using fortygige**	By default, a 40-GE interface is not split and operates as a single interface.

Configuring basic settings of an Ethernet interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the interface description.	**description** *text*	The default setting is in the format of *interface-name* **Interface**. For example, **GigabitEthernet1/0/1 Interface**.
4. Set the duplex mode of the Ethernet interface.	**duplex** { **auto** | **full** | **half** }	The default setting is **auto** for Ethernet interfaces. Copper ports operating at 1000 Mbps or 10 Gbps and fiber ports do not support the **half** keyword.
5. Set the port speed.	**speed** { **10** | **100** | **1000** | **10000** | **40000** | **auto** }	The default setting is **auto** for Ethernet interfaces. Support for the keywords depends on the interface type. For more information, see *Layer 2—LAN Switching Command*

Step	Command	Remarks
		Reference. Interfaces on an HPE 5130/5510 10GbE SFP+ 2-port Module (JH157A) or HPE 5130/5510 10GBASE-T 2-port Module (JH156A) interface card support only the **10000** keyword.
6. Configure the expected bandwidth of the interface.	**bandwidth** *bandwidth-value*	By default, the expected bandwidth (in kbps) is the interface baud rate divided by 1000.
7. Restore the default settings for the Ethernet interface.	**default**	N/A
8. Bring up the Ethernet interface.	**undo shutdown**	By default, Ethernet interfaces are in up state.

Configuring the link mode of an Ethernet interface

CAUTION:

After you change the link mode of an Ethernet interface, all commands (except the **shutdown** and **combo enable** commands) on the Ethernet interface are restored to their defaults in the new link mode.

The interfaces on this switch series can operate either as Layer 2 or Layer 3 Ethernet interfaces.

You can set the link mode to bridge or route.

To change the link mode of an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Change the link mode of the Ethernet interface.	**port link-mode** { **bridge** | **route** }	By default, Ethernet interfaces operate in bridge mode.

Configuring jumbo frame support

An Ethernet interface might receive some frames larger than the standard Ethernet frame size during high-throughput data exchanges, such as file transfers. These frames are called jumbo frames.

The interface processes jumbo frames in the following ways:

- When the Ethernet interface is configured to deny jumbo frames (by using the **undo jumboframe enable** command), the Ethernet interface discards jumbo frames without further processing.
- When the Ethernet interface is configured with jumbo frame support, the Ethernet interface performs the following operations:
  - Processes jumbo frames within the specified length.
  - Discards jumbo frames exceeding the specified length without further processing.

To configure jumbo frame support in interface view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure jumbo frame support.	**jumboframe enable** [*value*]	In Release 1111 and Release 1121, the switch allows jumbo frames within 10000 bytes to pass through all Ethernet interfaces by default. In Release 1122P02 and later, the switch allows jumbo frames within 12288 bytes to pass through all Ethernet interfaces by default.

Configuring physical state change suppression on an Ethernet interface

IMPORTANT:

Do not configure physical state change suppression on an Ethernet interface that has RRPP, MSTP, or Smart Link enabled.

The physical link state of an Ethernet interface is either up or down. Each time the physical link of a port comes up or goes down, the interface immediately reports the change to the CPU. The CPU then performs the following operations:

- Notifies the upper-layer protocol modules (such as routing and forwarding modules) of the change for guiding packet forwarding.
- Automatically generates traps and logs, informing the user to take the correct actions.

To prevent frequent physical link flapping from affecting system performance, configure physical state change suppression to suppress the reporting of physical link state changes. The system reports physical layer changes only when the suppression interval expires.

When the **link-delay** *delay-time* command is configured:

- The link-down event is not reported to the CPU unless the interface is still down when the suppression interval (*delay-time*) expires.
- The link-up event is immediately reported.

When the **link-delay** *delay-time* **mode up** command is configured:

- The link-up event is not reported to the CPU unless the interface is still up when the suppression interval (*delay-time*) expires.
- The link-down event is immediately reported.

When the **link-delay** *delay-time* **mode updown** command is configured:

- The link-down event is not reported to the CPU unless the interface is still down when the suppression interval (*delay-time*) expires.
- The link-up event is not reported to the CPU unless the interface is still up when the suppression interval (*delay-time*) expires.

To configure physical state change suppression on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure physical state change suppression on the interface.	**link-delay** [**msec**] *delay-time* [**mode** { **up** | **updown** }]	By default, the link-down or link-up event is immediately reported to the CPU. If you configure this command multiple times on an Ethernet interface, the most recent configuration takes effect.

Performing a loopback test on an Ethernet interface

If an Ethernet interface does not work correctly, you can perform a loopback test on it to identify the problem. An Ethernet interface in a loopback test does not forward data traffic.

Loopback tests include the following types:

- **Internal loopback test**—Tests all on-chip functions related to the Ethernet interface.
- **External loopback test**—Tests the hardware of the Ethernet interface. To perform an external loopback test on the Ethernet interface, connect a loopback plug to the Ethernet interface. The switch sends test packets out of the interface, which are expected to loop over the plug and back to the interface. If the interface fails to receive any test packets, the hardware of the interface is faulty.

Configuration restrictions and guidelines

- On an administratively shut down Ethernet interface (displayed as in **ADM** or **Administratively DOWN** state), you cannot perform an internal or external loopback test.
- The **speed**, **duplex**, **mdix-mode**, and **shutdown** commands are not available during a loopback test.
- During a loopback test, the Ethernet interface operates in full duplex mode. When a loopback test is complete, the port returns to its duplex setting.

Configuration procedure

To perform a loopback test on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Perform a loopback test.	**loopback** { **external** | **internal** }	By default, no loopback test is performed.

Configuring generic flow control on an Ethernet interface

CAUTION:

Configuring generic flow control on an Ethernet interface will cause link-up and link-down events before the interface finally stays up.

To avoid packet drops on a link, you can enable generic flow control at both ends of the link. When traffic congestion occurs at the receiving end, the receiving end sends a flow control (Pause) frame to ask the sending end to suspend sending packets.

- With TxRx mode generic flow control enabled, an interface can both send and receive flow control frames. When congestion occurs, the interface sends a flow control frame to its peer. When the interface receives a flow control frame from the peer, it suspends sending packets.
- With Rx flow mode generic control enabled, an interface can receive flow control frames, but it cannot send flow control frames. When the interface receives a flow control frame from its peer, it suspends sending packets to the peer. When congestion occurs, the interface cannot send flow control frames to the peer.

To handle unidirectional traffic congestion on a link, configure the **flow-control receive enable** command at one end and the **flow-control** command at the other end. To enable both ends of a link to handle traffic congestion, configure the **flow-control** command at both ends.

To enable generic flow control on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable generic flow control.	• Enable TxRx mode generic flow control: **flow-control** • Enable Rx mode generic flow control: **flow-control receive enable**	By default, generic flow control is disabled on an Ethernet interface.

Enabling energy saving features on an Ethernet interface

Enabling auto power-down on an Ethernet interface

IMPORTANT:

Fiber ports do not support this feature.

When the auto power-down feature is enabled on an interface and the interface has been down for a certain period of time, both of the following events occur:

- The switch automatically stops supplying power to the interface.
- The interface enters the power save mode.

The time period depends on the chip specifications and is not configurable.

When the interface comes up, both of the following events occur:

- The switch automatically restores power supply to the interface.
- The interface enters its normal state.

To enable auto power-down on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable auto power-down.	**port auto-power-down**	By default, auto power-down is disabled.

Enabling EEE energy saving for Ethernet interfaces in up state

IMPORTANT:

Fiber ports do not support this feature.

With the Energy Efficient Ethernet (EEE) energy saving feature, a link-up port enters the low power state if it has not received any packet for a certain period of time. The time period depends on the chip specifications and is not configurable. When a packet arrives later, the switch automatically restores power supply to the interface and the port enters the normal state.

To enable EEE energy saving:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable EEE energy saving.	**eee enable**	By default, EEE energy saving is disabled.

Setting the statistics polling interval

To set the statistics polling interval in Ethernet interface view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the statistics polling interval.	**flow-interval** *interval*	By default, the statistics polling interval is 300 seconds.

To display the interface statistics collected in the last polling interval, use the **display interface** command.

To clear interface statistics, use the **reset counters interface** command.

Configuring the interface card operating mode

IMPORTANT:

This feature is applicable only to HPE 5510 48G 4SFP+ HI 1-slot Switch (JH146A) and HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch (JH148A).

An interface card can operate in one of the following operating modes:

- **0**—All interfaces on the interface card are not available, and interfaces GigabitEthernet 1/0/41 through GigabitEthernet 1/0/48 on the front panel are available.
- **1**—Interfaces numbered 5 through 8 on the interface card are not available, and the following interfaces are available:
  - Interfaces numbered 1 through 4 on the interface card.
  - Interfaces GigabitEthernet 1/0/41 through GigabitEthernet 1/0/48 on the front panel.
- **2**—Interfaces GigabitEthernet 1/0/41 through GigabitEthernet 1/0/48 on the front panel are not available, and all interfaces on the interface card are available.

For HPE 5510 48G 4SFP+ HI 1-slot Switch and HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch, the operating modes supported by the interface cards are as shown in Table 1.

Table 1 Operating modes supported by interface cards

Interface card	Supported operating modes	Remarks
HPE 5510 2-port QSFP+ Module (JH155A)	**0** and **2**.	The operating modes take effect only on 10-GE breakout interfaces split from a QSFP+ interface.

After you configure the interface card operating mode, reboot the switch to make the configuration take effect.

You can view the interface card operating mode information by using the **display port-configuration-mode status** command.

To configure the interface card operating mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the interface card operating mode.	**port-configuration-mode slot** *slot-number* { **0** | **1** | **2** }	By default, the operating mode of the interface card is **0**.

Enabling automatic negotiation for speed downgrading

Perform this task to enable interfaces at two ends of a link to automatically negotiate about downgrading their speed when the following conditions exist:

- The interfaces automatically negotiate a speed of 1000 Mbps.
- The interfaces cannot operate at 1000 Mbps because of link restrictions.

This command is applicable only to GE interfaces.

To enable automatic negotiation for speed downgrading:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable automatic negotiation for speed downgrading.	**speed auto downgrade**	By default, automatic negotiation for speed downgrading is enabled.

Configuring a Layer 2 Ethernet interface

Configuring storm suppression

You can use the storm suppression feature to limit the size of a particular type of traffic (broadcast, multicast, or unknown unicast traffic) on an interface. When the broadcast, multicast, or unknown unicast traffic on the interface exceeds this threshold, the system discards packets until the traffic drops below this threshold.

Any of the **storm-constrain**, **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands can suppress storm on a port. The **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands suppress traffic in hardware. They have less impact on device performance than the **storm-constrain** command, which performs suppression in software.

Configuration guidelines

For the same type of traffic, do not configure the **storm constrain** command together with any of the **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands. Otherwise, the traffic suppression result is not determined. For more information about the **storm-constrain** command, see "Configuring storm control on an Ethernet interface."

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.
- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

For the suppression threshold that takes effect, see the prompt on the switch.

Configuration procedure

To set storm suppression thresholds on one or multiple Ethernet interfaces:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable broadcast suppression and set the broadcast suppression threshold.	**broadcast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	By default, broadcast traffic is allowed to pass through an interface.
4. Enable multicast suppression and set the multicast suppression threshold.	**multicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	By default, multicast traffic is allowed to pass through an interface.
5. Enable unknown unicast suppression and set the unknown unicast suppression threshold.	**unicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	By default, unknown unicast traffic is allowed to pass through an interface.

Configuring storm control on an Ethernet interface

IMPORTANT:

The known unicast storm control feature is available in Release 1121 and later.

Storm control compares broadcast, multicast, unknown unicast traffic, and known unicast traffic regularly with their respective traffic thresholds on an Ethernet interface. For each type of traffic, storm control provides a lower threshold and a higher threshold.

For management purposes, you can configure the interface to output threshold event traps and log messages when monitored traffic meets one of the following conditions:

- Exceeds the upper threshold.
- Falls below the lower threshold from the upper threshold.

Depending on your configuration, when a particular type of traffic exceeds its upper threshold, the interface does either of the following:

- **Blocks this type of traffic, while forwarding other types of traffic**—Even though the interface does not forward the blocked traffic, it still counts the traffic. When the blocked traffic drops below the lower threshold, the port begins to forward the traffic.
- **Goes down automatically**—The interface goes down automatically and stops forwarding any traffic. When the blocked traffic is detected dropping below the lower threshold, the port does not forward the traffic. To bring up the interface, use the **undo shutdown** command or disable the storm control feature.

Any of the **storm-constrain**, **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands can suppress storm on a port. The **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands suppress traffic in hardware, and have less impact on device performance than the **storm-constrain** command, which performs suppression in software.

Storm control uses a complete polling cycle to collect traffic data, and analyzes the data in the next cycle. An interface takes one to two polling intervals to take a storm control action.

Configuration guidelines

For the same type of traffic, do not configure the **storm constrain** command together with any of the **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands. Otherwise, the traffic suppression result is not determined. For more information about the **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands, see "Configuring storm suppression."

Configuration procedure

To configure storm control on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Set the traffic polling interval of the storm control module.	**storm-constrain interval** *seconds*	The default setting is 10 seconds. For network stability, use the default or set a higher traffic polling interval (10 seconds).
3. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. (Optional.) Enable storm control, and set the lower and upper thresholds for broadcast, multicast, or unknown unicast traffic.	**storm-constrain** { **broadcast** | **known-unicast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *max-pps-values min-pps-values*	By default, storm control is disabled. The **known-unicast** key word is available in Release 1121 and later.
5. Set the control action to take when monitored traffic exceeds the upper threshold.	**storm-constrain control** { **block** | **shutdown** }	By default, storm control is disabled.
6. (Optional.) Enable the interface to log storm control threshold events.	**storm-constrain enable log**	By default, the interface outputs log messages when monitored traffic exceeds the upper threshold or falls below the lower threshold from the upper threshold.
7. (Optional.) Enable the interface to send storm control threshold event traps.	**storm-constrain enable trap**	By default, the interface sends traps when monitored traffic exceeds the upper threshold or drops below the lower threshold

Step	Command	Remarks
		from the upper threshold.

Forcibly bringing up a fiber port

CAUTION:

The following operations on a fiber port will cause link updown events before the port finally stays up:

- Configure the **port up-mode** command and the **speed** or **duplex** command at the same time.
- Install or remove fiber links or transceiver modules after you forcibly bring up the fiber port.

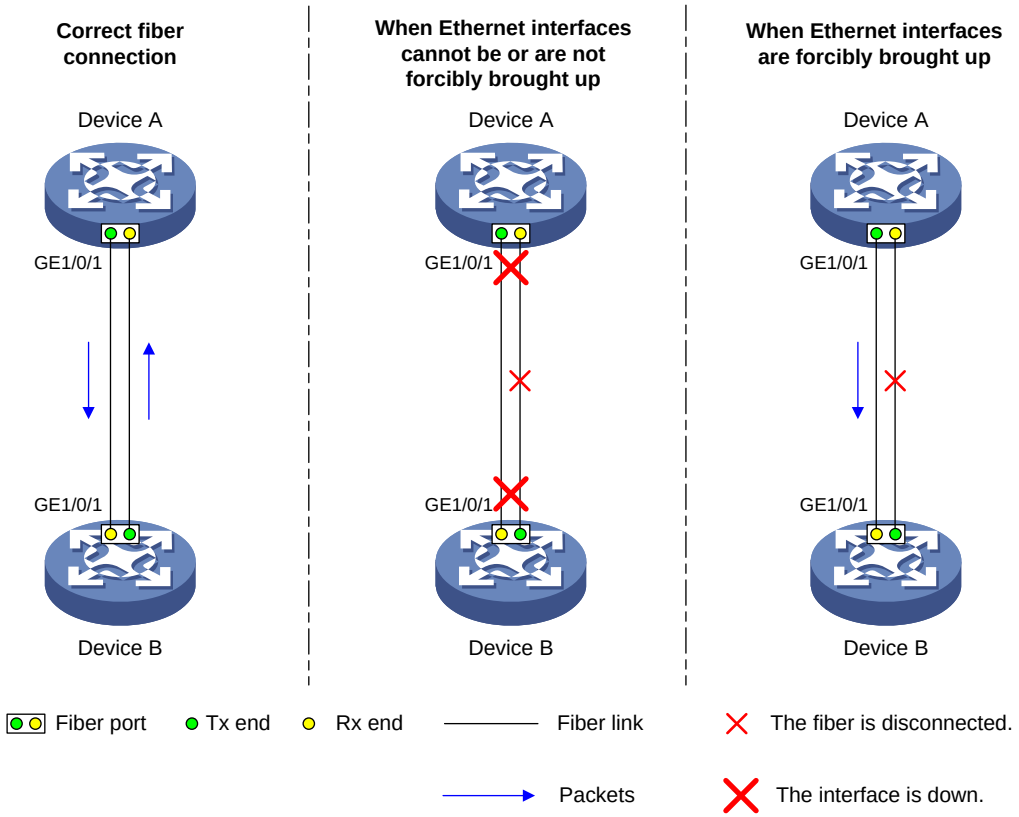
IMPORTANT:

Copper ports do not support this feature.

As shown in Figure 1, a fiber port typically uses separate fibers for transmitting and receiving packets. The physical state of the fiber port is up only when both transmit and receive fibers are physically connected. If one of the fibers is disconnected, the fiber port does not work.

To enable a fiber port to forward traffic over a single link, you can use the **port up-mode** command. This command brings up a fiber port by force, even when no fiber links or optical modules are present. If one fiber link is present and up, the fiber port can forward packets over the link unidirectionally.

Figure 1 Forcibly bring up a fiber port



Configuration restrictions and guidelines

When you forcibly bring up a fiber port, follow these guidelines:

- The **port up-mode** command is mutually exclusive with either of the **shutdown** and commands.
- A GE fiber port cannot correctly forward traffic if you configure the **port up-mode** command on the port and install an electro-optical module, 100/1000-Mbps transceiver module, or 100-Mbps transceiver module into the port. To solve the problem, use the **undo port up-mode** command on the fiber port.

Configuration procedure

To forcibly bring up a fiber port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Forcibly bring up the fiber port.	**port up-mode**	By default, a fiber Ethernet port is not forcibly brought up, and the physical state of a fiber port depends on the physical state of the fibers.

Setting the MDIX mode of an Ethernet interface

IMPORTANT:

Fiber ports do not support the MDIX mode setting.

A physical Ethernet interface contains eight pins, each of which plays a dedicated role. For example, pins 1 and 2 transmit signals, and pins 3 and 6 receive signals. You can use both crossover and straight-through Ethernet cables to connect copper Ethernet interfaces. To accommodate these types of cables, a copper Ethernet interface can operate in one of the following Medium Dependent Interface-Crossover (MDIX) modes:

- **MDIX mode**—Pins 1 and 2 are receive pins and pins 3 and 6 are transmit pins.
- **MDI mode**—Pins 1 and 2 are transmit pins and pins 3 and 6 are receive pins.
- **AutoMDIX mode**—The interface negotiates pin roles with its peer.

To enable the interface to communicate with its peer, set the MDIX mode of the interface mode by using the following guidelines:

- Typically, set the MDIX mode of the interface to AutoMDIX. Set the MDIX mode of the interface to MDI or MDIX only when the switch cannot determine the cable type.
- When a straight-through cable is used, set the interface to operate in the MDIX mode different than its peer.
- When a crossover cable is used, perform either of the following tasks:
  - Set the interface to operate in the same MDIX mode as its peer.
  - Set either end to operate in AutoMDIX mode.

To set the MDIX mode of an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A

Step	Command	Remarks
3. Set the MDIX mode of the Ethernet interface.	**mdix-mode** { **automdix** | **mdi** | **mdix** }	By default, a copper Ethernet interface operates in auto mode to negotiate pin roles with its peer.

Testing the cable connection of an Ethernet interface

IMPORTANT:

- If the link of an Ethernet port is up, testing its cable connection will cause the link to go down and then come up.
- Fiber ports do not support this feature.

This feature tests the cable connection of an Ethernet interface and displays cable test results within 5 seconds. The test results include the cable's status and some physical parameters. If any fault is detected, the test results include the length of the faulty cable segment.

To test the cable connection of an Ethernet interface:

Step	Command
1. Enter system view.	**system-view**
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*
3. Test the cable connected to the Ethernet interface.	**virtual-cable-test**

Enabling bridging on an Ethernet interface

When a packet arrives at an interface, the switch looks up the destination MAC address of the packet in the MAC address table. If an entry is found and the outgoing interface is the same as the incoming interface, the switch drops the packet.

To enable the switch to forward such packets rather than drop them, enable the bridging feature on the Ethernet interface.

To enable bridging on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable bridging on the Ethernet interface.	**port bridge enable**	By default, bridging is disabled.

Configuring a Layer 3 Ethernet interface

Setting the MTU for an Ethernet interface

The value of maximum transmission unit (MTU) affects the fragmentation and reassembly of IP packets. Typically, you do not need to modify the MTU of an interface.

To set the MTU for an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the MTU.	**mtu** *size*	The default setting is 1500 bytes.

Displaying and maintaining an Ethernet interface

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display interface traffic statistics.	**display counters** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
Display traffic rate statistics of interfaces in up state over the last sampling interval.	**display counters rate** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
Display the operational and status information of the specified interface or all interfaces.	**display interface** [*interface-type* [*interface-number*]]
Display summary information about the specified interface or all interfaces.	**display interface** [*interface-type* [*interface-number*]] **brief** [**description**]
Display information about dropped packets on the specified interface or all interfaces.	**display packet-drop** { **interface** [*interface-type* [*interface-number*]] | **summary** }
Display information about storm control on the specified interface or all interfaces. (Available in Release 1111.)	**display storm-constrain** [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]
Display information about storm control on the specified interface or all interfaces. (Available in Release 1121 and later.)	**display storm-constrain** [**broadcast | known-unicast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]
Display interface card operating mode information. (Applicable only to HPE 5510 48G 4SFP+ HI 1-slot Switch and HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch.)	**display port-configuration-mode status**
Display the Ethernet statistics.	**display ethernet statistics slot** *slot-number*
Clear the interface statistics.	**reset counters interface** [*interface-type* [*interface-number*]]
Clear the statistics of dropped packets on the specified interfaces.	**reset packet-drop interface** [*interface-type* [*interface-number*]]
Clear the Ethernet statistics.	**reset ethernet statistics**

Configuring loopback, null, and inloopback interfaces

This chapter describes how to configure a loopback interface, a null interface, and an inloopback interface.

Configuring a loopback interface

A loopback interface is a virtual interface. The physical layer state of a loopback interface is always up unless the loopback interface is manually shut down. Because of this benefit, loopback interfaces are widely used in the following scenarios:

- **Configuring a loopback interface address as the source address of the IP packets that the device generates**—Because loopback interface addresses are stable unicast addresses, they are usually used as device identifications.
  - When you configure a rule on an authentication or security server to permit or deny packets that a device generates, you can simplify the rule by configuring it to permit or deny packets carrying the loopback interface address that identifies the device.
  - When you use a loopback interface address as the source address of IP packets, make sure the route from the loopback interface to the peer is reachable by performing routing configuration. All data packets sent to the loopback interface are considered packets sent to the device itself, so the device does not forward these packets.
- **Using a loopback interface in dynamic routing protocols**—With no router ID configured for a dynamic routing protocol, the system selects the highest loopback interface IP address as the router ID. In BGP, to avoid interruption of BGP sessions due to physical port failure, you can use a loopback interface as the source interface of BGP packets.

To configure a loopback interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a loopback interface and enter loopback interface view.	**interface loopback** *interface-number*	N/A
3. Set the interface description.	**description** *text*	The default setting is *interface name* **Interface** (for example, **LoopBack1 Interface**).
4. Configure the expected bandwidth of the loopback interface.	**bandwidth** *bandwidth-value*	By default, the expected bandwidth of a loopback interface is 0 kbps.
5. Restore the default settings for the loopback interface.	**default**	N/A
6. Bring up the loopback interface.	**undo shutdown**	By default, a loopback interface is up.

Configuring a null interface

A null interface is a virtual interface and is always up, but you cannot use it to forward data packets or configure it with an IP address or link layer protocol. The null interface provides a simpler way to filter packets than ACL. You can filter undesired traffic by transmitting it to a null interface instead of

applying an ACL. For example, if you specify a null interface as the next hop of a static route to a network segment, any packets routed to the network segment are dropped.

To configure a null interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter null interface view.	**interface null 0**	Interface Null 0 is the default null interface on the device and cannot be manually created or removed. Only one null interface, Null 0, is supported on the device. The null interface number is always 0.
3. Set the interface description.	**description** *text*	The default setting is NULL0 Interface.
4. Restore the default settings for the null interface.	**default**	N/A

Configuring an inloopback interface

An inloopback interface is a virtual interface created by the system, which cannot be configured or deleted. The physical layer and link layer protocol states of an inloopback interface are always up. All IP packets sent to an inloopback interface are considered packets sent to the device itself and are not forwarded.

Displaying and maintaining loopback, null, and inloopback interfaces

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information about the specified or all loopback interfaces.	**display interface** [**loopback** [*interface-number*]] [**brief** [**description**]] **display interface** [**loopback**] [**brief** [**down**]]
Display information about the null interface.	**display interface** [**null** [**0**]] [**brief** [**description**]]
Display information about the inloopback interface.	**display interface** [**inloopback** [**0**]] [**brief** [**description**]]
Clear the statistics on the specified or all loopback interfaces.	**reset counters interface loopback** [*interface-number*]
Clear the statistics on the null interface.	**reset counters interface** [**null** [**0**]]

Bulk configuring interfaces

You can enter interface range view to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, you can execute the **shutdown** command in interface range view to shut down a range of interfaces.

Configuration restrictions and guidelines

When you bulk configure interfaces in interface range view, follow these restrictions and guidelines:

- In interface range view, only the commands supported by the first interface are available. The first interface is specified with the **interface range** command.
- If you cannot enter the view of an interface by using the **interface** *interface-type interface-number* command, do not configure the interface as the first interface in the interface range.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands might break up the aggregation after they are executed on both an aggregate interface and its member interfaces.
- No limit is set on the maximum number of interfaces in an interface range. The more interfaces in an interface range, the longer the command execution time.
- The maximum number of interface range names is limited only by the system resources. To guarantee bulk interface configuration performance, configure fewer than 1000 interface range names.
- After a command is executed in interface range view, one of the following situations might occur:
  - The system stays in interface range view and does not display an error message. It means that the execution succeeded on all member interfaces in the interface range.
  - The system displays an error message and stays in interface range view. It means that the execution failed on member interfaces in the interface range.
    - If the execution failed on the first member interface in the interface range, the command is not executed on any member interfaces.
    - If the execution failed on non-first member interfaces, the command takes effect on the other member interfaces.
  - The system returns to system view. It means that:
    - The command is supported in both system view and interface view.
    - The execution failed on a member interface in interface range view and succeeded in system view.
    - The command is not executed on the subsequent member interfaces.

    You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

Configuration procedure

To bulk configure interfaces:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter interface range view.	• **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> • **interface range name** *name* [**interface** { int*erface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	By using the **interface range name** command, you assign a name to an interface range and can specify this name rather than the interface range to enter the interface range view.
3. (Optional.) Display commands available for the first interface in the interface range.	Enter a question mark (?) at the interface range prompt.	N/A
4. Use available commands to configure the interfaces.	Available commands vary by interface.	N/A
5. (Optional.) Verify the configuration.	**display this**	N/A

Displaying and maintaining bulk interface configuration

Execute the **display** command in any view.

Task	Command
Display information about the interface ranges that are configured by using the **interface range name** command.	**display interface range** [**name** *name*]

Configuring the MAC address table

Overview

An Ethernet device uses a MAC address table to forward frames. A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID. When the device receives a frame, it uses the destination MAC address of the frame to look for a match in the MAC address table.

- The device forwards the frame out of the outgoing interface in the matching entry if a match is found.
- The device floods the frame in the VLAN of the frame if no match is found.

How a MAC address entry is created

The entries in the MAC address table include entries automatically learned by the device and entries manually added.

MAC address learning

The device can automatically populate its MAC address table by learning the source MAC addresses of incoming frames on each interface.

When a frame arrives at an interface (for example, port A), the device performs the following operations:

1. Checks the source MAC address (for example, MAC-SOURCE) of the frame.
2. Looks up the source MAC address in the MAC address table.
   - The device updates the entry if an entry is found.
   - The device adds an entry for MAC-SOURCE and port A if no entry is found.
3. When the device receives a frame destined for MAC-SOURCE after learning this source MAC address, the device performs the following operations:
   a. Finds the MAC-SOURCE entry in the MAC address table.
   b. Forwards the frame out of port A.

The device performs the learning process each time it receives a frame with an unknown source MAC address until the table is fully populated.

Manually configuring MAC address entries

Dynamic MAC address learning does not distinguish between illegitimate and legitimate frames, which can invite security hazards. When Host A is connected to port A, a MAC address entry will be learned for the MAC address of Host A (for example, MAC A). When an illegal user sends frames with MAC A as the source MAC address to port B, the device performs the following operations:

1. Learns a new MAC address entry with port B as the outgoing interface and overwrites the old entry for MAC A.
2. Forwards frames destined for MAC A out of port B to the illegal user.

As a result, the illegal user obtains the data of Host A. To improve the security for Host A, manually configure a static entry to bind Host A to port A. Then, the frames destined for Host A are always sent out of port A. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

Types of MAC address entries

A MAC address table can contain the following types of entries:

- **Static entries**—A static entry is manually added to forward frames with a specific destination MAC address out of the associated interface, and it never ages out. A static entry has higher priority than a dynamically learned one.
- **Dynamic entries**—A dynamic entry can be manually configured or dynamically learned to forward frames with a specific destination MAC address out of the associated interface. A dynamic entry might age out. A manually configured dynamic entry has the same priority as a dynamically learned one.
- **Blackhole entries**—A blackhole entry is manually configured and never ages out. A blackhole entry is configured for filtering out frames with a specific source or destination MAC address. For example, for security purposes, to block all frames destined for or sourced from a user, you can configure the user's MAC address as a blackhole MAC address entry.
- **Multiport unicast entries**—A multiport unicast entry is manually added to send frames with a specific unicast destination MAC address out of multiple ports, and it never ages out. A multiport unicast entry has higher priority than a dynamically learned one.

A static, blackhole, or multiport unicast MAC address entry can overwrite a dynamic MAC address entry, but not vice versa.

MAC address table configuration task list

The configuration tasks discussed in the following sections can be performed in any order.

This document covers only the configuration of unicast MAC address entries, including static, dynamic, blackhole, and multiport unicast MAC address entries. For information about configuring static multicast MAC address entries, see *IP Multicast Configuration Guide*. For information about MAC address table configuration in VPLS, see *MPLS Configuration Guide*.

To configure the MAC address table, perform the following tasks:

Tasks at a glance
(Optional.) Configuring MAC address entries • Adding or modifying a static or dynamic MAC address entry globally • Adding or modifying a static or dynamic MAC address entry on an interface • Adding or modifying a blackhole MAC address entry • Adding or modifying a multiport unicast MAC address entry
(Optional.) Disabling MAC address learning
(Optional.) Configuring the aging timer for dynamic MAC address entries
(Optional.) Configuring the MAC learning limit on an interface
(Optional.) Configuring the device to forward unknown frames after the MAC learning limit on an interface is reached
(Optional.) Assigning MAC learning priority to an interface
(Optional.) Enabling MAC address synchronization
(Optional.) Enable MAC address move notifications
(Optional.) Enabling ARP fast update for MAC address moves
(Optional.) Enabling SNMP notifications for the MAC address table

Configuring MAC address entries

Configuration guidelines

- You cannot add a dynamic MAC address entry if a learned entry already exists with a different outgoing interface for the MAC address.
- The manually configured static, blackhole, and multiport unicast MAC address entries cannot survive a reboot if you do not save the configuration. The manually configured dynamic MAC address entries are lost upon reboot whether or not you save the configuration.

A frame whose source MAC address matches different types of MAC address entries is processed differently.

Type	Description
Static MAC address entry	• Discards the frame received on a different interface from that in the entry. • Forwards the frame received on the same interface with that in the entry.
Multiport unicast MAC address entry	• Learns the MAC address (for example, MAC A) of the frame, generates a dynamic MAC address entry for MAC A, and forwards the frame. However, the generated dynamic MAC address entry does not take effect. Frames destined for MAC A are forwarded based on the multiport unicast MAC address entry.
Dynamic MAC address entry	• Learns the MAC address of the frames received on a different interface from that in the entry and overwrites the original entry. • Forwards the frame received on the same interface as that in the entry and updates the aging timer for the entry.

Adding or modifying a static or dynamic MAC address entry globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Add or modify a static or dynamic MAC address entry.	**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	By default, no MAC address entry is configured globally. Make sure you have created the VLAN and assigned the interface to the VLAN.

Adding or modifying a static or dynamic MAC address entry on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number*	N/A

Step	Command	Remarks
	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	
3. Add or modify a static or dynamic MAC address entry.	**mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*	By default, no MAC address entry is configured on an interface. Make sure you have created the VLAN and assigned the interface to the VLAN.

Adding or modifying a blackhole MAC address entry

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Add or modify a blackhole MAC address entry.	**mac-address blackhole** *mac-address* **vlan** *vlan-id*	By default, no blackhole MAC address entry is configured. Make sure you have created the VLAN.

Adding or modifying a multiport unicast MAC address entry

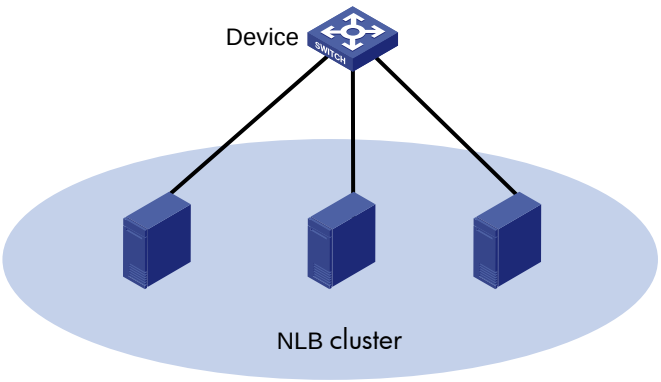
You can configure a multiport unicast MAC address entry to associate a unicast destination MAC address with multiple ports. The frame with a destination MAC address matching the entry is sent out of multiple ports.

For example, in NLB unicast mode:

- All servers within the cluster uses the cluster's MAC address as their own address.
- Frames destined for the cluster are forwarded to every server in the group.

In this case, you can configure a multiport unicast MAC address entry on the device connected to the server group. Then, the device forwards the frame destined for the server group through all ports connected to the servers within the cluster.

Figure 2 NLB cluster



Do not configure an interface as the output interface of a multiport unicast MAC address entry if the interface receives frames destined for the multiport unicast MAC address. Otherwise, the frames are flooded on the VLAN to which they belong.

You can configure a multiport unicast MAC address entry globally or on an interface.

Configuring a multiport unicast MAC address entry globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Add or modify a multiport unicast MAC address entry.	**mac-address multiport** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	By default, no multiport unicast MAC address entry is configured globally. Make sure you have created the VLAN and assigned the interface to the VLAN.

Configuring a multiport unicast MAC address entry on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Add the interface to a multiport unicast MAC address entry.	**mac-address multiport** *mac-address* **vlan** *vlan-id*	By default, no multiport unicast MAC address entry is configured on an interface. Make sure you have created the VLAN and assigned the interface to the VLAN.

Disabling MAC address learning

MAC address learning is enabled by default. To prevent the MAC address table from being saturated when the device is experiencing attacks, disable MAC address learning. For example, you can disable MAC address learning to prevent the device from being attacked by a large amount of frames with different source MAC addresses.

When MAC address learning is disabled, the device immediately deletes the existing dynamic MAC address entries.

Disabling global MAC address learning

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable global MAC address learning.	**undo mac-address mac-learning enable**	By default, global MAC address learning is enabled.

Disabling global MAC address learning disables MAC address learning on all interfaces.

The global MAC address learning configuration does not take effect in a VPLS VSI. For information about VSIs, see *MPLS Configuration Guide*.

Disabling MAC address learning on an interface

When global MAC address learning is enabled, you can disable MAC address learning on a single interface.

To disable MAC address learning on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Disable MAC address learning on the interface.	**undo mac-address mac-learning enable**	By default, MAC address learning on the interface is enabled.

Disabling MAC address learning on a VLAN

When global MAC address learning is enabled, you can disable MAC address learning on a per-VLAN basis.

To disable MAC address learning on a VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable global MAC address learning.	**mac-address mac-learning enable**	By default, global MAC address learning is enabled.
3. Enter VLAN view.	**vlan** *vlan-id*	N/A
4. Disable MAC address learning on the VLAN.	**undo mac-address mac-learning enable**	By default, MAC address learning on the VLAN is enabled.

Configuring the aging timer for dynamic MAC address entries

For security and efficient use of table space, the MAC address table uses an aging timer for each dynamic MAC address entry. If a dynamic MAC address entry is not updated before the aging timer expires, the device deletes the entry. This aging mechanism ensures that the MAC address table can promptly update to accommodate latest network topology changes.

A stable network requires a longer aging interval, and an unstable network requires a shorter aging interval.

An aging interval that is too long might cause the MAC address table to retain outdated entries. As a result, the MAC address table resources might be exhausted, and the MAC address table might fail to update to accommodate the latest network changes.

An interval that is too short might result in removal of valid entries, which would cause unnecessary floods and possibly affect the device performance.

To reduce floods on a stable network, set a long aging timer or disable the timer to prevent dynamic entries from unnecessarily aging out. Reducing floods improves the network performance. Reducing flooding also improves the security because it reduces the chances for a data frame to reach unintended destinations.

To configure the aging timer for dynamic MAC address entries:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the aging timer for dynamic MAC address entries.	**mac-address timer** { **aging** *seconds* | **no-aging** }	By default, the aging timer for dynamic MAC address entries is 300 seconds The **no-aging** keyword disables the aging timer.

Configuring the MAC learning limit on an interface

This feature limits the MAC address table size. A large MAC address table will degrade forwarding performance..

To configure the MAC learning limit on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the MAC learning limit on the interface.	**mac-address max-mac-count** *count*	By default, the maximum number of MAC addresses that can be learned on an interface is not configured.

Configuring the device to forward unknown frames after the MAC learning limit on an interface is reached

In this document, unknown frames refer to frames whose source MAC addresses are not in the MAC address table.

You can enable or disable forwarding of unknown frames after the MAC learning limit is reached.

To enable the interface to forward unknown frames after the MAC learning limit is reached:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter interface view.	• Enter Layer 2 Ethernet interface view. **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view. **interface bridge-aggregation** *interface-number*	N/A
3. Configure the device to forward unknown frames received on the interface after the MAC learning limit on the interface is reached.	**mac-address max-mac-count enable-forwarding**	By default, the device can forward unknown frames received on an interface after the MAC learning limit on the interface is reached.

Assigning MAC learning priority to an interface

IMPORTANT:

To make this feature take effect in an IRF fabric, you must also enable MAC address synchronization by using the **mac-address mac-roaming enable** command.

The MAC learning priority mechanism assigns either low priority or high priority to an interface. An interface with high priority can learn MAC addresses as usual. However, an interface with low priority is not allowed to learn MAC addresses already learned on a high-priority interface.

The MAC learning priority mechanism can help defend your network against MAC address spoofing attacks. In a network that performs MAC-based forwarding, an upper layer device MAC address might be learned by a downlink interface because of a loop or attack to the downlink interface. To avoid this problem, perform the following tasks:

- Assign high MAC learning priority to an uplink interface.
- Assign low MAC learning priority to a downlink interface.

To assign MAC learning priority to an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Assign MAC learning priority to the interface.	**mac-address mac-learning priority** { **high** | **low** }	By default, low MAC learning priority is used.

Enabling MAC address synchronization

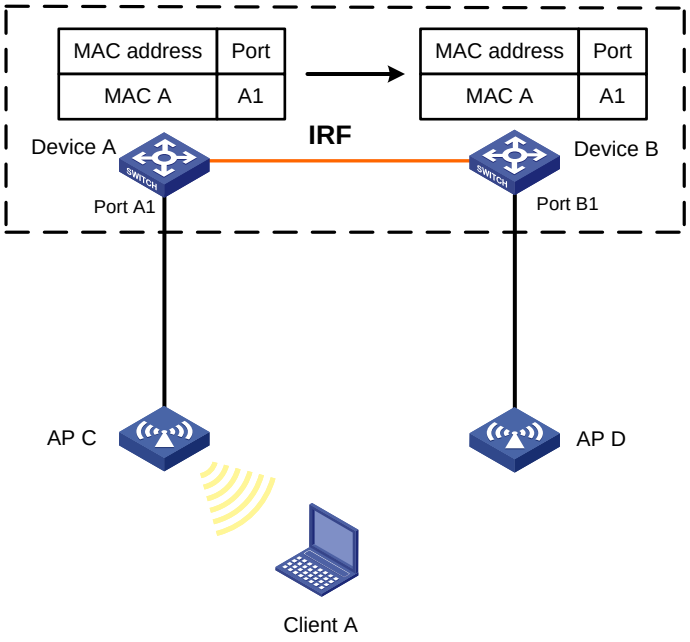
To avoid unnecessary floods and improve forwarding speed, make sure all member devices have the same MAC address table. After you enable MAC address synchronization, each member device advertises learned MAC address entries to other member devices.

As shown in Figure 3,

- Device A and Device B form an IRF fabric enabled with MAC address synchronization.
- Device A and Device B connect to AP C and AP D, respectively.

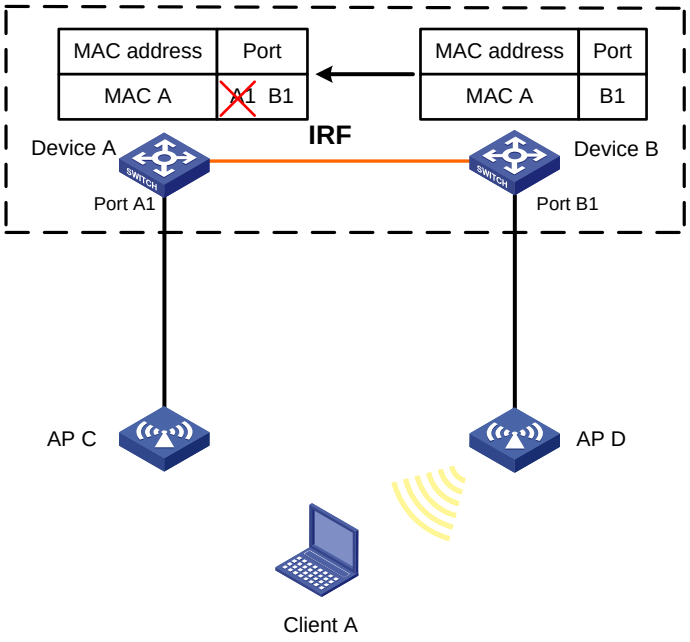
When Client A associates with AP C, Device A learns a MAC address entry for Client A and advertises it to Device B.

Figure 3 MAC address tables of devices when Client A accesses AP C



When Client A roams to AP D, Device B learns a MAC address entry for Client A. Device B advertises it to Device A to ensure service continuity for Client A, as shown in Figure 4.

Figure 4 MAC address tables of devices when Client A roams to AP D



To enable MAC address synchronization:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MAC address synchronization.	**mac-address mac-roaming enable**	By default, MAC address synchronization is disabled.

Enable MAC address move notifications

The outgoing interface for a MAC address entry learned on interface A is changed to interface B when the following conditions exist:

- Interface B receives a packet with the MAC address as the source MAC address.
- Interface B belongs to the same VLAN as interface A.

In this case, the MAC address is moved from interface A to interface B, and a MAC address move occurs.

If a MAC address is continuously moved between the two interfaces, Layer 2 loops might occur.. To detect and locate loops, you can view the MAC address move information.

When the system detects that a MAC address frequently moves from an interface, you can configure MAC address move suppression on the interface to bring it down. The interface can automatically come up after waiting for the specified suppression interval. Or, you can manually bring up the interface. To make MAC address move suppression take effect, you must use this feature together with ARP fast update. For more information about ARP fast update, see "Enabling ARP fast update for MAC address moves."

To display the MAC address move records after the device is started, use the **display mac-address mac-move** command.

To enable MAC address move notifications:

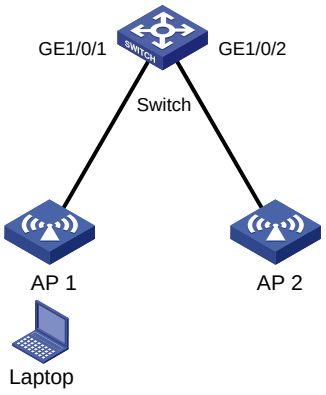
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MAC address move notifications and optionally specify a detection interval.	**mac-address notification mac-move** [**interval** *interval-value*]	By default, MAC address move notifications are disabled. If you do not specify a detection interval, the default setting of 1 minute is used. After you execute this command, the system sends only log messages to the information center module. If the device is also configured with the **snmp-agent trap enable mac-address** command, the system also sends SNMP notifications to the SNMP module.
3. Set a threshold for MAC address moves sourced from an interface within a detection interval.	**mac-address notification mac-move suppression threshold** *threshold-value*	The default setting is 3.
4. Set a MAC address move suppression interval.	**mac-address notification mac-move suppression interval** *interval-value*	The default setting is 30 seconds.
5. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
6. Enable MAC address move suppression.	**mac-address notification mac-move suppression**	By default, MAC address move suppression is disabled.
7. Return to system view.	**quit**	N/A
8. Enable ARP fast update for MAC address moves.	**mac-address mac-move fast-update**	This task is required when you enable MAC address move suppression. By default, ARP fast update for MAC address moves is disabled.

Enabling ARP fast update for MAC address moves

ARP fast update for MAC address moves allows the device to update an ARP entry immediately after the outgoing interface for a MAC address changes. This feature ensures data connection without interruption.

As shown in Figure 5, a mobile user Laptop accesses the network by connecting to AP 1 or AP 2. When the AP to which the user connects changes, the switch updates the ARP entry for the user immediately after it detects a MAC address move.

Figure 5 ARP fast update application scenario



To enable ARP fast update for MAC address moves:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable ARP fast update for MAC address moves.	**mac-address mac-move fast-update**	By default, ARP fast update for MAC address moves is disabled.

Enabling SNMP notifications for the MAC address table

After you enable SNMP notifications for the MAC address table, the device will send SNMP notifications to the SNMP module to notify the NMS of important events. You can set the notification sending parameters in SNMP to determine the attributes of sending notifications.

After you disable SNMP notifications for the MAC address table, the device will only send log messages to the information center module. You can set the output rules and destinations to examine the log messages of the MAC address table module.

For more information about SNMP notifications and information center, see *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for the MAC address table:

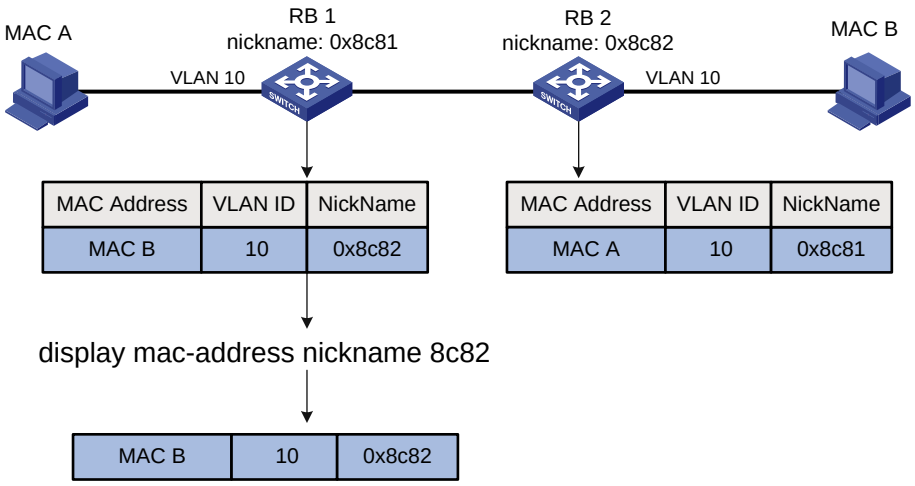
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications for the MAC address table.	**snmp-agent trap enable mac-address** [**mac-move**]	By default, SNMP notifications are disabled for the MAC address table.

Displaying and maintaining the MAC address table

Execute **display** commands in any view.

Task	Command
Display MAC address table information.	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole** | **multiport**] [**vlan** *vlan-id*] [**count**]]
Display the aging timer for dynamic MAC address entries.	**display mac-address aging-time**
Display the system or interface MAC address learning state.	**display mac-address mac-learning** [**interface** *interface-type interface-number*]
Display MAC address statistics.	**display mac-address statistics**
Display the MAC address move records.	**display mac-address mac-move** [**slot** *slot-number*]

Figure 6 An example for the display mac-address nickname command



MAC address table configuration example

Network requirements

Host A at MAC address 000f-e235-dc71 is connected to interface GigabitEthernet 1/0/1 of Device and belongs to VLAN 1.

Host B at MAC address 000f-e235-abcd, which behaved suspiciously on the network, also belongs to VLAN 1.

Configure the MAC address as follows:

- To prevent MAC address spoofing, add a static entry for Host A in the MAC address table of Device.
- To drop all frames destined for Host B, add a blackhole MAC address entry for the host.
- Set the aging timer to 500 seconds for dynamic MAC address entries.

Configuration procedure

Add a static MAC address entry for MAC address 000f-e235-dc71 on GigabitEthernet 1/0/1 that belongs to VLAN 1.

```
<Device> system-view
[Device] mac-address static 000f-e235-dc71 interface gigabitethernet 1/0/1 vlan 1
```

Add a blackhole MAC address entry for MAC address 000f-e235-abcd that belongs to VLAN 1.

```
[Device] mac-address blackhole 000f-e235-abcd vlan 1
```

Set the aging timer to 500 seconds for dynamic MAC address entries.

```
[Device] mac-address timer aging 500
```

Verifying the configuration

Display the static MAC address entries for interface GigabitEthernet 1/0/1.

```
[Device] display mac-address static interface gigabitethernet 1/0/1
MAC Address      VLAN ID    State            Port/NickName            Aging
000f-e235-dc71   1          Static           GE1/0/1                  N
```

Display the blackhole MAC address entries.

```
[Device] display mac-address blackhole
MAC Address      VLAN ID    State            Port/NickName            Aging
000f-e235-abcd   1          Blackhole        N/A                      N
```

Display the aging time of dynamic MAC address entries.

```
[Device] display mac-address aging-time
MAC address aging time: 500s.
```

Configuring MAC Information

The MAC Information feature can generate syslog messages or SNMP notifications when MAC address entries are learned or deleted. You can use these messages to monitor users leaving or joining the network and analyze network traffic.

The MAC Information feature buffers the MAC change syslog messages or SNMP notifications in a queue. The device overwrites the oldest MAC address change written into the queue with the most recent MAC address change when the following conditions exist:

- The MAC change notification interval does not expire.
- The queue has been exhausted.

To send a syslog message or SNMP notification immediately after it is created, set the queue length to zero.

The device writes information and sends messages only for the following MAC addresses:

- Dynamic MAC addresses.
- MAC addresses that pass MAC authentication.
- MAC addresses that pass 802.1X authentication.
- Secure MAC addresses.

The device does not write information or send messages for blackhole MAC addresses, static MAC addresses, multiport unicast MAC addresses, multicast MAC addresses, and local MAC addresses.

For more information about MAC authentication, 802.1X, and secure MAC addresses, see *Security Configuration Guide*.

Enabling MAC Information

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MAC Information globally.	**mac-address information enable**	By default, MAC Information is globally disabled.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Enable MAC Information on the interface.	**mac-address information enable** { **added** | **deleted** }	By default, MAC Information is disabled on an interface. Make sure you have enabled MAC Information globally before you enable it on the interface.

Configuring the MAC Information mode

The following MAC Information modes are available for sending MAC address changes:

- **Syslog**—The device sends syslog messages to notify MAC address changes. The device sends syslog messages to the information center, which then outputs them to the monitoring terminal. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

- **Trap**—The device sends SNMP notifications to notify MAC address changes. The device sends SNMP notifications to the NMS. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

To configure the MAC Information mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the MAC Information mode.	**mac-address information mode** { **syslog** | **trap** }	The default setting is **trap**.

Configuring the MAC change notification interval

To prevent syslog messages or SNMP notifications from being sent too frequently, you can set the MAC change notification interval to a larger value.

To set the MAC change notification interval:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the MAC change notification interval.	**mac-address information interval** *interval-time*	The default setting is 1 second.

Configuring the MAC Information queue length

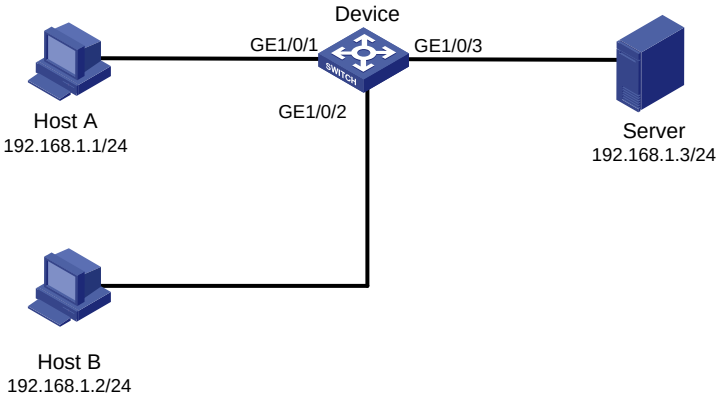
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the MAC Information queue length.	**mac-address information queue-length** *value*	The default setting is 50.

MAC Information configuration example

Network requirements

Enable MAC Information on interface GigabitEthernet 1/0/1 on Device in Figure 7 to send MAC address changes in syslog messages to the log host, Host B, through interface GigabitEthernet 1/0/2.

Figure 7 Network diagram



Configuration restrictions and guidelines

When you edit the file **/etc/syslog.conf**, follow these restrictions and guidelines:

- Comments must be on a separate line and must begin with a pound sign (#).
- No redundant spaces are allowed after the file name.
- The logging facility name and the severity level specified in the **/etc/syslog.conf** file must be the same as those configured on the device. Otherwise, the log information might not be output correctly to the log host. The logging facility name and the severity level are configured by using the **info-center loghost** and **info-center source** commands, respectively.

Configuration procedure

1. Configure Device to send syslog messages to Host B:

   # Enable the information center.

   ```
   <Device> system-view
   [Device] info-center enable
   ```

   # Specify the log host 192.168.1.2/24 and specify **local4** as the logging facility.

   ```
   [Device] info-center loghost 192.168.1.2 facility local4
   ```

   # Disable log output to the log host.

   ```
   [Device] info-center source default loghost deny
   ```

   To avoid output of unnecessary information, disable all modules from outputting logs to the specified destination (**loghost**, in this example) before you configure an output rule.

   # Configure an output rule to output to the log host MAC address logs that have a severity level of at least **informational**.

   ```
   [Device] info-center source mac loghost level informational
   ```

2. Configure the log host, Host B:

   Configure Solaris as follows. Configure other UNIX operating systems in the same way Solaris is configured.

   a. Log in to the log host as a root user.

   b. Create a subdirectory named **Device** in directory **/var/log/**.

   ```
   # mkdir /var/log/Device
   ```

   c. Create file **info.log** in the **Device** directory to save logs from **Device**.

   ```
   # touch /var/log/Device/info.log
   ```

   d. Edit the file **syslog.conf** in directory **/etc/** and add the following contents:

```
# Device configuration messages
local4.info /var/log/Device/info.log
```

In this configuration, **local4** is the name of the logging facility that the log host uses to receive logs, and **info** is the informational level. The UNIX system records the log information that has a severity level of at least **informational** to the file **/var/log/Device/info.log**.

e. Display the process ID of **syslogd**, end the **syslogd** process, and then restart **syslogd** using the **–r** option to make the new configuration take effect.

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

The device can output MAC address logs to the log host, which stores the logs to the specified file.

3. Enable MAC Information on Device:

Enable MAC Information globally.

```
[Device] mac-address information enable
```

Configure the MAC Information mode as syslog.

```
[Device] mac-address information mode syslog
```

Enable MAC Information on interface GigabitEthernet 1/0/1 to enable GigabitEthernet 1/0/1 to record MAC address change information when the interface performs either of the following operations:

- Learns a new MAC address.
- Deletes an existing MAC address.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-address information enable added
[Device-GigabitEthernet1/0/1] mac-address information enable deleted
[Device-GigabitEthernet1/0/1] quit
```

Set the MAC Information queue length to 100.

```
[Device] mac-address information queue-length 100
```

Set the MAC change notification interval to 20 seconds.

```
[Device] mac-address information interval 20
```

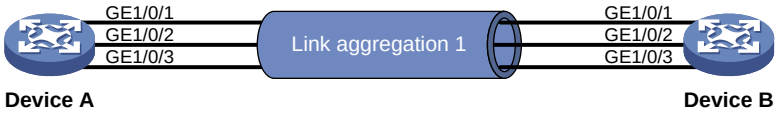
Configuring Ethernet link aggregation

Ethernet link aggregation bundles multiple physical Ethernet links into one logical link, called an aggregate link. Link aggregation has the following benefits:

- Increased bandwidth beyond the limits of any single link. In an aggregate link, traffic is distributed across the member ports.
- Improved link reliability. The member ports dynamically back up one another. When a member port fails, its traffic is automatically switched to other member ports.

As shown in Figure 8, Device A and Device B are connected by three physical Ethernet links. These physical Ethernet links are combined into an aggregate link called link aggregation 1. The bandwidth of this aggregate link can reach up to the total bandwidth of the three physical Ethernet links. At the same time, the three Ethernet links back up one another. When a physical Ethernet link fails, the traffic previously carried on the failed link is switched to the other two links.

Figure 8 Ethernet link aggregation diagram



Basic concepts

Aggregation group, member port, and aggregate interface

Link bundling is implemented through interface bundling. An aggregation group is a group of Ethernet interfaces bundled together, which are called member ports of the aggregation group. For each aggregation group, a logical interface (called an aggregate interface), is created. When an upper layer entity uses the link aggregation service, the following events occur:

- A link aggregation group appears the same as a single logical link.
- An aggregate interface transmits data traffic.

When you create an aggregate interface, the device automatically creates an aggregation group of the same type and number as the aggregate interface. For example, when you create aggregate interface 1, aggregation group 1 is created.

Aggregate interfaces include Layer 2 aggregate interfaces and Layer 3 aggregate interfaces.

You can assign Layer 2 Ethernet interfaces only to a Layer 2 aggregation group, and Layer 3 Ethernet interfaces only to a Layer 3 aggregation group.

NOTE:

You can use the **port link-mode** command to configure an Ethernet port as a Layer 2 or Layer 3 interface (see "Configuring Ethernet interfaces").

The port rate of an aggregate interface equals the total rate of its Selected member ports. Its duplex mode is the same as that of the Selected member ports. For more information about the states of member ports in an aggregation group, see "Aggregation states of member ports in an aggregation group."

Aggregation states of member ports in an aggregation group

A member port in an aggregation group can be in any of the following aggregation states:

- **Selected**—A Selected port can forward traffic.
- **Unselected**—An Unselected port cannot forward traffic.
- **Individual**—An Individual port can forward traffic as a normal physical port. A port is placed in the Individual state when the following conditions are met:
  - The corresponding aggregate interface is configured as an edge aggregate interface.
  - The port does not receive LACPDUs from its peer port.

Operational key

When aggregating ports, the system automatically assigns each port an operational key based on port information, such as port rate and duplex mode. Any change to this information triggers a recalculation of the operational key.

In an aggregation group, all Selected ports are assigned the same operational key.

Configuration types

Every configuration setting on a port might affect its aggregation state. Port configurations include the following types:

- **Attribute configurations**—To become a Selected port, a member port must have the same attribute configurations as the aggregate interface. Table 2 describes the attribute configurations.

  Attribute configurations made on an aggregate interface are automatically synchronized to all member ports. These configurations are retained on the member ports even after the aggregate interface is removed.

  Any attribute configuration change on a member port might affect the aggregation states and running services of the member ports. The system displays a warning message every time you try to change an attribute configuration setting on a member port.

  Table 2 Attribute configurations

Feature	Considerations
Port isolation	Indicates whether the port has joined an isolation group, and which isolation group the port belongs to.
QinQ	QinQ enable state (enabled/disabled), TPID for VLAN tags, and VLAN transparent transmission. For information about QinQ, see "Configuring QinQ."
VLAN mapping	Different types of VLAN mapping configured on the port. For more information about VLAN mapping, see "Configuring VLAN mapping."
VLAN	VLAN attribute configurations include the following: • Permitted VLAN IDs. • PVID. • Link type (trunk, hybrid, or access). • Operating mode (promiscuous, trunk promiscuous, host). • VLAN tagging mode. For information about VLAN, see "Configuring VLANs."

- **Protocol configurations**—Protocol configurations do not affect the aggregation state of the member ports. MAC address learning and spanning tree settings are examples of protocol configurations.

NOTE:

The protocol configuration for a member port is effective only when the member port leaves the aggregation group.

Link aggregation modes

Link aggregation has dynamic and static modes:

- **Static aggregation mode**—Aggregation is stable. The aggregation state of the member ports are not affected by the peer ports.
- **Dynamic aggregation mode**—The peering system automatically maintains the aggregation state of the member ports, which reduces the administrators' workload.

An aggregation group in static mode is called a "static aggregation group" and an aggregation group in dynamic mode is called a "dynamic aggregation group."

Aggregating links in static mode

Choosing a reference port

When setting the aggregation state of the ports in an aggregation group, the system automatically chooses a member port as the reference port. A Selected port must have the same operational key and attribute configurations as the reference port.

The system chooses a reference port from the member ports that are in up state with the same attribute configurations as the aggregate interface.

The candidate ports are sorted in the following order:

1. Highest port priority
2. Full duplex/high speed
3. Full duplex/low speed
4. Half duplex/high speed
5. Half duplex/low speed

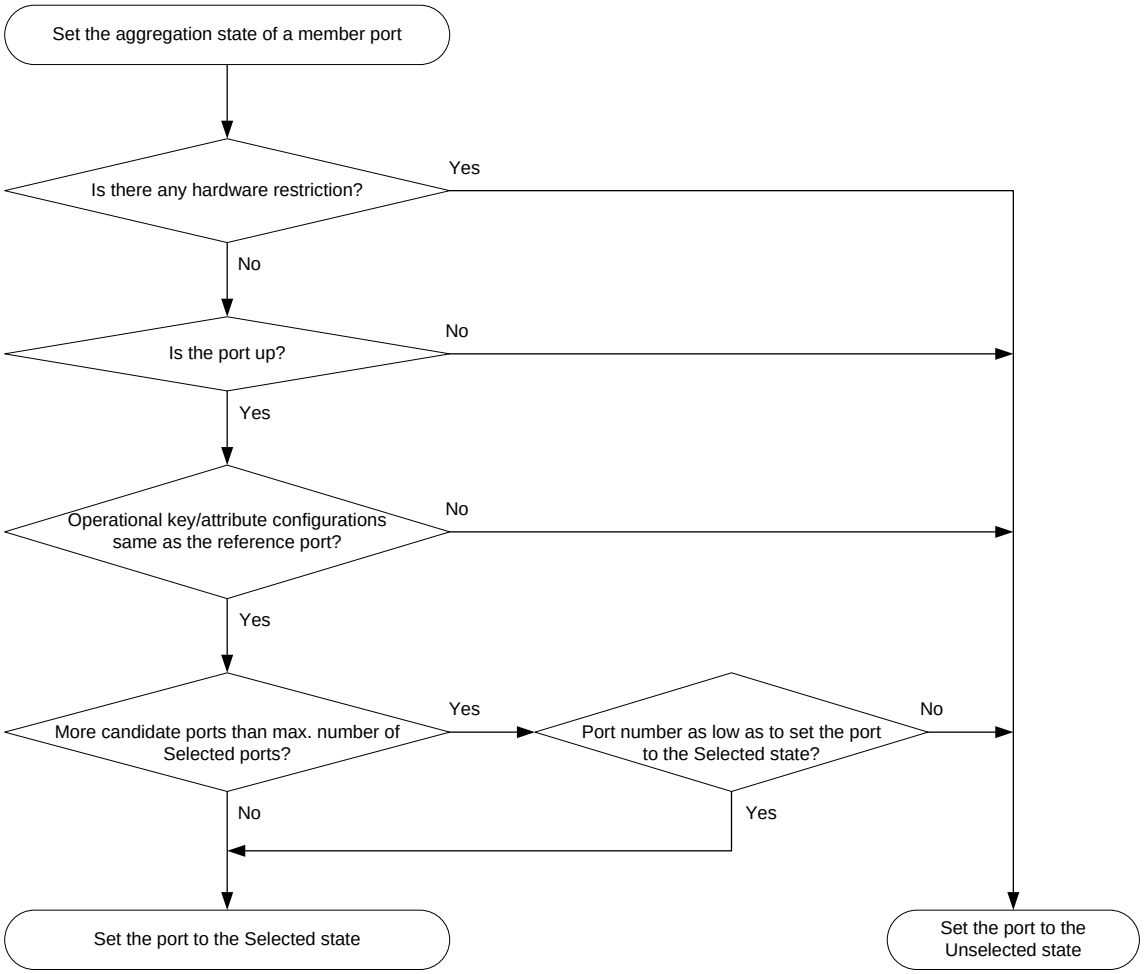
The candidate port at the top is chosen as the reference port.

- If multiple ports have the same port priority, duplex mode, and speed, the port that has been a Selected port (if any) is chosen. If multiple ports have been Selected ports, the one with the smallest port number is chosen.
- If multiple ports have the same port priority, duplex mode, and speed and none of them has been a Selected port, the port with the smallest port number is chosen.

Setting the aggregation state of each member port

After a static aggregation group reaches the limit on Selected ports, ports attempting to join the group are put in Unselected state. This prevents traffic interruption on the existing Selected ports.

Figure 9 Setting the aggregation state of a member port in a static aggregation group



For more information about configuring the maximum number of Selected ports in a static aggregation group, see "Setting the minimum and maximum numbers of Selected ports for an aggregation group."

Any operational key or attribute configuration change might affect the aggregation states of link aggregation member ports and ongoing traffic.

Aggregating links in dynamic mode

Dynamic aggregation mode is implemented through IEEE 802.3ad Link Aggregation Control Protocol (LACP).

LACP

LACP uses LACPDUs to exchange aggregation information between LACP-enabled devices.

Each member port in an LACP-enabled aggregation group exchanges information with its peer. When a member port receives an LACPDU, it compares the received information with information received on the other member ports. In this way, the two systems reach an agreement on which ports are placed in the Selected state.

LACP functions

LACP offers basic LACP functions and extended LACP functions, as described in Table 3.

Table 3 Basic and extended LACP functions

Category	Description
Basic LACP functions	Implemented through the basic LACPDU fields, including the system LACP priority, system MAC address, port priority, port number, and operational key.
Extended LACP functions	Implemented by extending the LACPDU with new TLV fields. This is how the LACP MAD mechanism of the IRF feature is implemented. The switch series can participate in LACP MAD as either an IRF member device or an intermediate device. For more information about IRF and the LACP MAD mechanism, see *IRF Configuration Guide*.

LACP operating modes

LACP can operate in active mode or passive mode.

When LACP is operating in passive mode on a local member port and its peer port, both ports cannot send LACPDUs. When LACP is operating in active mode on the port on either end of a link, both ports can send LACPDUs.

LACP priorities

LACP priorities include system LACP priority and port priority, as described in Table 4. The smaller the priority value, the higher the priority.

Table 4 LACP priorities

Type	Description
System LACP priority	Used by two peer devices (or systems) to determine which one is superior in link aggregation. In dynamic link aggregation, the system that has higher system LACP priority sets the Selected state of member ports on its side. The system that has lower priority sets the aggregation state of local member ports the same as their respective peer ports.
Port priority	Determines the likelihood of a member port to be selected on a system. A port with a higher port priority is more likely to become Selected.

LACP timeout interval

The LACP timeout interval specifies how long a member port waits to receive LACPDUs from the peer port. If a local member port does not receive LACPDUs from the peer within the LACP timeout interval, the member port considers the peer as failed.

The LACP timeout interval also determines the LACPDU sending rate of the peer. LACP timeout intervals include the following types:

- **Short timeout interval**—3 seconds. If you use the short timeout interval, the peer sends one LACPDU per second.
- **Long timeout interval**—90 seconds. If you use the long timeout interval, the peer sends one LACPDU every 30 seconds.

How dynamic link aggregation works

Choosing a reference port

The system chooses a reference port from the member ports that are in up state and have the same attribute configurations as the aggregate interface. A Selected port must have the same operational key and attribute configurations as the reference port.

The local system (the actor) and the remote system (the partner) negotiate a reference port by using the following workflow:

1. The two systems determine the system with the smaller system ID.

   A system ID contains the system LACP priority and the system MAC address.

   a. The two systems compare their LACP priority values.

      The lower the LACP priority, the smaller the system ID. If the LACP priority values are the same, the two systems proceed to step b.

   b. The two systems compare their MAC addresses.

      The lower the MAC address, the smaller the system ID.

2. The system with the smaller system ID chooses the port with the smallest port ID as the reference port.

   A port ID contains a port priority and a port number. The lower the port priority, the smaller the port ID.

   a. The system chooses the port with the lowest priority value as the reference port.

      If the ports have the same priority, the system proceeds to step b.

   b. The system compares their port numbers.

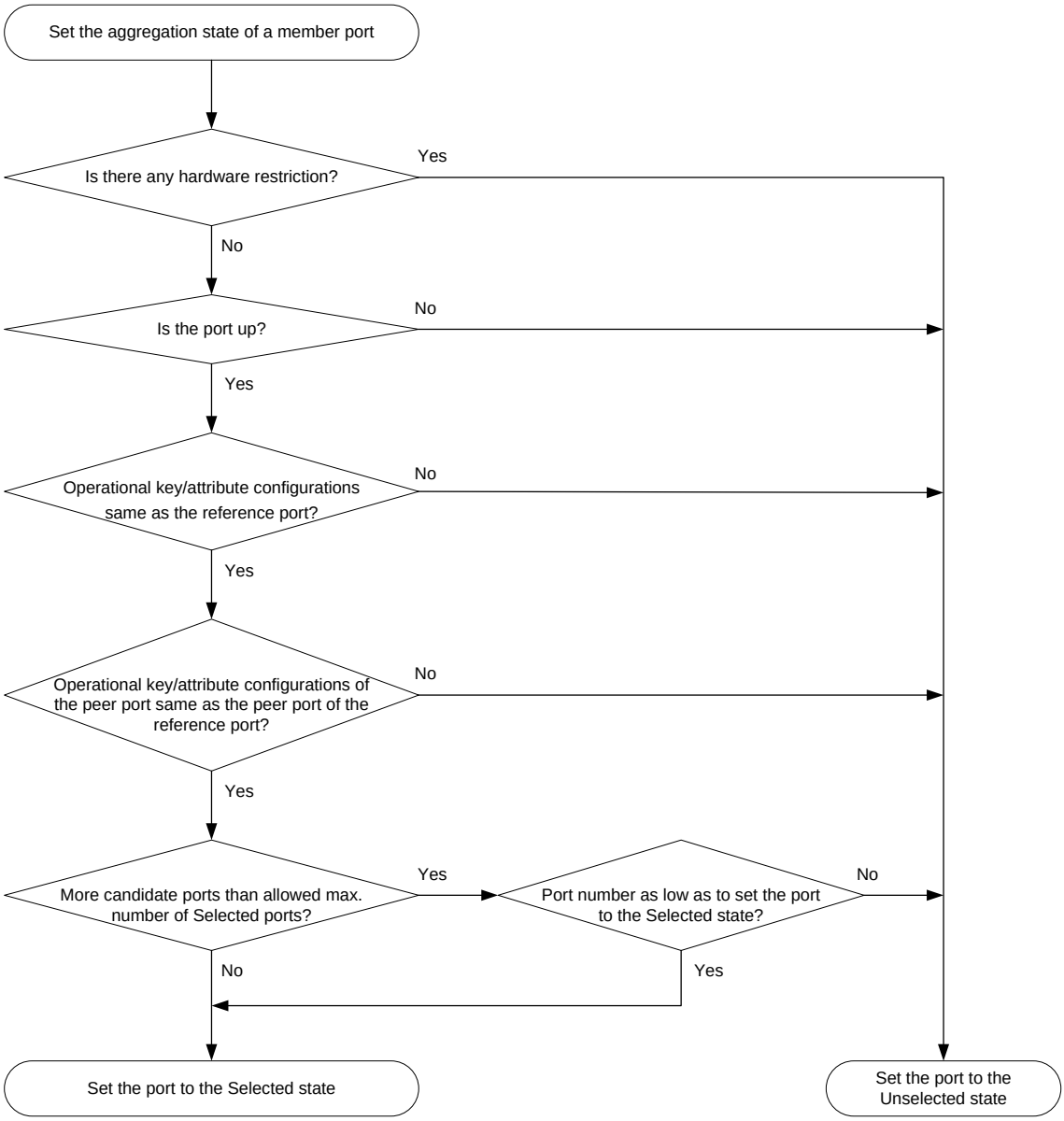
      The smaller the port number, the smaller the port ID.

      The port with the smallest port number and the same attribute configurations as the aggregate interface is chosen as the reference port.

Setting the aggregation state of each member port

After the reference port is chosen, the system with the smaller system ID sets the state of each member port on its side.

Figure 10 Setting the state of a member port in a dynamic aggregation group



The system with the higher system ID is aware of the aggregation state changes on the remote system. The system sets the aggregation state of local member ports the same as their peer ports.

When you aggregate interfaces in dynamic mode, follow these guidelines:

- A dynamic link aggregation group preferably chooses full-duplex ports as the Selected ports. The group chooses only one half-duplex port as a Selected port when either of the following conditions exist:
  - None of the full-duplex ports can become Selected ports.
  - Only half-duplex ports exist in the group.
- To ensure stable aggregation and service continuity, do not change the operational key or attribute configurations on any member port.
- When the aggregation state of a local port changes in a dynamic aggregation group, the aggregation state of the peer port also changes.
- After the Selected port limit has been reached, a port joining the aggregation group is placed in the Selected state if it is more eligible than a current member port.

For more information about configuring the maximum number of Selected ports in a dynamic aggregation group, see "Setting the minimum and maximum numbers of Selected ports for an aggregation group."

Edge aggregate interface

Dynamic link aggregation fails on a server-facing aggregate interface if dynamic link aggregation is configured only on the device. The device forwards traffic by using only one of the physical ports that are connected to the server.

To improve link reliability, configure the aggregate interface as an edge aggregate interface. This feature enables all member ports of the aggregation group to forward traffic. When a member port fails, its traffic is automatically switched to other member ports.

After dynamic link aggregation is configured on the server, the device can receive LACPDUs from the server. Then, link aggregation between the device and the server operates correctly.

An edge aggregate interface takes effect only when it is configured on an aggregate interface corresponding to a dynamic aggregation group.

Load sharing modes for link aggregation groups

In a link aggregation group, traffic can be load shared across the Selected ports based on any of the following modes:

- **Per-flow load sharing**—Load shares traffic on a per-flow basis. The load sharing mode classifies packets into flows and forwards packets of the same flow on the same link. This mode can be one or any combination of the following criteria that classify traffic:
  - Source or destination MAC address.
  - Source or destination port number.
  - Ingress port.
  - Source or destination IP address.
- **Packet type-based load sharing**—Load shares traffic automatically based on packet types (Layer 2, IPv4, or IPv6 for example).

Ethernet link aggregation configuration task list

Tasks at a glance
(Required.) Configuring an aggregation group: • Configuring a static aggregation group • Configuring a dynamic aggregation group
(Optional.) Configuring an aggregate interface: • Configuring the description of an aggregate interface • Specifying ignored VLANs for a Layer 2 aggregate interface • Setting the MTU for a Layer 3 aggregate interface • Setting the minimum and maximum numbers of Selected ports for an aggregation group • Setting the expected bandwidth for an aggregate interface • Configuring an edge aggregate interface • Enabling BFD for an aggregation group • Shutting down an aggregate interface • Restoring the default settings for an aggregate interface

Tasks at a glance
(Optional.) Configuring load balancing for link aggregation group: • Setting load sharing modes for link aggregation groups • Enabling local-first load sharing for link aggregation • Configuring per-flow load sharing algorithm settings for Ethernet link aggregation
Enabling link-aggregation traffic redirection
Specifying link aggregation management VLANs and management port

Configuring an aggregation group

This section explains how to configure an aggregation group.

Configuration restrictions and guidelines

When you configure an aggregation group, follow these restrictions and guidelines:

- You cannot assign a port to a Layer 2 aggregation group if any of the following features are configured on the port:
  - MAC authentication. (See *Security Configuration Guide*.)
  - Port security. (See *Security Configuration Guide*.)
  - 802.1X. (See *Security Configuration Guide*.)
  - Association between AC and cross connection. (See *MPLS Configuration Guide*.)
  - AC-VSI association. (See *MPLS Configuration Guide*.)
- You cannot assign a port to a Layer 3 aggregation group if any of the following features are configured on the port:
  - Association between AC and cross connection. (See *MPLS Configuration Guide*.)
  - AC-VSI association. (See *MPLS Configuration Guide*.)
- If a port is used as a reflector port for port mirroring, do not assign it to an aggregation group. For more information about reflector ports, see *Network Management and Monitoring Configuration Guide*.
- Removing an aggregate interface also removes its aggregation group and causes all member ports to leave the aggregation group.
- You must configure the same aggregation mode on the two ends of an aggregate link.
- This switch series supports a maximum of 128 aggregation groups. To ensure the operation of the service loopback groups, configure no more than 126 aggregation groups.

Configuring a static aggregation group

To guarantee a successful static aggregation, make sure that the ports at both ends of each link are in the same aggregation state.

Avoid assigning ports to a static aggregation group that has reached the limit on Selected ports. These ports will be placed in the Unselected state to avoid traffic interruption on the current Selected ports. However, a device reboot can cause the aggregation state of member ports to change.

Configuring a Layer 2 static aggregation group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.	**interface bridge-aggregation** *interface-number*	When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 static aggregation group numbered the same.
3. Exit to system view.	**quit**	N/A
4. Assign an interface to the specified Layer 2 aggregation group.	**a.** Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* **b.** Assign the interface to the specified Layer 2 aggregation group: **port link-aggregation group** *number*	Repeat these two sub-steps to assign more Layer 2 Ethernet interfaces to the aggregation group.

Configuring a Layer 3 static aggregation group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a Layer 3 aggregate interface and enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	When you create a Layer 3 aggregate interface, the system automatically creates a Layer 3 static aggregation group numbered the same.
3. Exit to system view.	**quit**	N/A
4. Assign an interface to the specified Layer 3 aggregation group.	**a.** Enter Layer 3 Ethernet interface view: **interface** *interface-type interface-number* **b.** Assign the interface to the specified Layer 3 aggregation group: **port link-aggregation group** *number*	Repeat these two sub-steps to assign more Layer 3 Ethernet interfaces to the aggregation group.

Configuring a dynamic aggregation group

To guarantee a successful dynamic aggregation, make sure that the peer ports of the ports aggregated at one end are also aggregated. The two ends can automatically negotiate the aggregation state of each member port.

Configuring a Layer 2 dynamic aggregation group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the system LACP priority.	**lacp system-priority** *system-priority*	By default, the system LACP priority is 32768. Changing the system LACP priority might affect the aggregation state of the ports in a

Step	Command	Remarks
		dynamic aggregation group.
3. Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.	**interface bridge-aggregation** *interface-number*	When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 static aggregation group numbered the same.
4. Configure the aggregation group to operate in dynamic aggregation mode.	**link-aggregation mode dynamic**	By default, an aggregation group operates in static aggregation mode.
5. Exit to system view.	**quit**	N/A
6. Assign an interface to the specified Layer 2 aggregation group.	**a.** Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* **b.** Assign the interface to the specified Layer 2 aggregation group: **port link-aggregation group** *number*	Repeat these two sub-steps to assign more Layer 2 Ethernet interfaces to the aggregation group.
7. Set the LACP operating mode for the interface.	• Set LACP to operate in passive mode: **lacp mode passive** • Set LACP to operate in active mode: **undo lacp mode**	By default, LACP is operating in active mode.
8. Configure the port priority for the interface.	**link-aggregation port-priority** *port-priority*	The default setting is 32768.
9. Set the short LACP timeout interval (3 seconds) for the interface.	**lacp period short**	By default, the long LACP timeout interval (90 seconds) is adopted by the interface. The peer sends LACPDUs slowly.

Configuring a Layer 3 dynamic aggregation group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the system LACP priority.	**lacp system-priority** *system-priority*	By default, the system LACP priority is 32768. Changing the system LACP priority might affect the aggregation state of the ports in the dynamic aggregation group.
3. Create a Layer 3 aggregate interface and enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	When you create a Layer 3 aggregate interface, the system automatically creates a Layer 3 static aggregation group numbered the same.
4. Configure the aggregation group to operate in dynamic aggregation mode.	**link-aggregation mode dynamic**	By default, an aggregation group operates in static aggregation mode.
5. Exit to system view.	**quit**	N/A

Step	Command	Remarks
6. Assign an interface to the specified Layer 3 aggregation group.	**a.** Enter Layer 3 Ethernet interface view: **interface** *interface-type interface-number* **b.** Assign the interface to the specified Layer 3 aggregation group: **port link-aggregation group** *number*	Repeat these two sub-steps to assign more Layer 3 Ethernet interfaces to the aggregation group.
7. Set the LACP operating mode for the interface.	• Set LACP to operate in passive mode: **lacp mode passive** • Set LACP to operate in active mode: **undo lacp mode**	By default, LACP is operating in active mode.
8. Configure the port priority for the interface.	**link-aggregation port-priority** *port-priority*	The default setting is 32768.
9. Set the short LACP timeout interval (3 seconds) for the interface.	**lacp period short**	By default, the long LACP timeout interval (90 seconds) is adopted by the interface. The peer sends LACPDUs slowly.

Configuring an aggregate interface

Most configurations that can be made on Layer 2 or Layer 3 Ethernet interfaces can also be made on Layer 2 or Layer 3 aggregate interfaces.

Configuring the description of an aggregate interface

You can configure the description of an aggregate interface for administration purposes, for example, describing the purpose of the interface.

To configure the description of an aggregate interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Configure the description of the aggregate interface.	**description** *text*	By default, the description of an interface is *interface-name* **Interface**.

Specifying ignored VLANs for a Layer 2 aggregate interface

By default, to become Selected ports, the member ports must have the same VLAN permit state and VLAN tagging mode as the corresponding Layer 2 aggregate interface.

The system ignores the permit state and tagging mode of an ignored VLAN when choosing Selected ports.

To specify ignored VLANs for a Layer 2 aggregate interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 aggregate interface view.	**interface bridge-aggregation** *interface-number*	N/A
3. Specify ignored VLANs.	**link-aggregation ignore vlan** *vlan-id-list*	By default, a Layer 2 aggregate interface does not ignore any VLANs.

Setting the MTU for a Layer 3 aggregate interface

The MTU of an interface affects IP packets fragmentation and reassembly on the interface.

To set the MTU for a Layer 3 aggregate interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	N/A
3. Set the MTU for the Layer 3 aggregate interface.	**mtu** *size*	The default setting is 1500 bytes.

Setting the minimum and maximum numbers of Selected ports for an aggregation group

IMPORTANT:

The minimum and maximum numbers of Selected ports must be the same for the local and peer aggregation groups.

The bandwidth of an aggregate link increases as the number of Selected member ports increases. To avoid congestion, you can set the minimum number of Selected ports required for bringing up an aggregate interface.

This minimum threshold setting affects the aggregation state of both aggregation member ports and the aggregate interface.

- When the number of member ports eligible to be Selected ports is smaller than the minimum threshold:
  - All member ports are placed in Unselected state.
  - The link of the aggregate interface goes down.
- When the minimum threshold is reached, the eligible member ports are placed in the Selected state, and the link of the aggregate interface goes up.

The maximum number of Selected ports allowed in an aggregation group is limited by either manual configuration or hardware limitation, whichever value is smaller.

You can implement backup between two ports by performing the following tasks:

- Assigning two ports to an aggregation group.
- Setting the maximum number of Selected ports to 1 for the aggregation group.

Then, only one Selected port is allowed in the aggregation group, and the Unselected port acts as a backup port.

To set the minimum and maximum numbers of Selected ports for an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Set the minimum number of Selected ports for the aggregation group.	**link-aggregation selected-port minimum** *number*	By default, the minimum number of Selected ports is not specified for an aggregation group.
4. Set the maximum number of Selected ports for the aggregation group.	**link-aggregation selected-port maximum** *number*	By default, the maximum number of Selected ports for an aggregation group is 32.

Setting the expected bandwidth for an aggregate interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Set the expected bandwidth for the interface.	**bandwidth** *bandwidth-value*	By default, the expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Configuring an edge aggregate interface

When you configure an edge aggregate interface, follow these restrictions and guidelines:

- This configuration takes effect only on the aggregate interface corresponding to a dynamic aggregation group.
- Link-aggregation traffic redirection does not operate correctly on an edge aggregate interface. For more information about link-aggregation traffic redirection, see "Enabling link-aggregation traffic redirection."

To configure an edge aggregate interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Configure the aggregate interface as an edge aggregate interface.	**lacp edge-port**	By default, an aggregate interface does not operate as an edge aggregate interface.

Enabling BFD for an aggregation group

BFD for Ethernet link aggregation can monitor member link status in an aggregation group. After you enable BFD on an aggregate interface, each Selected port in the aggregation group establishes a BFD session with its peer port. BFD operates differently depending on the aggregation mode.

- **BFD for static aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. The local port is placed in Unselected state. The BFD session between the local and peer ports remains, and the local port keeps sending BFD packets. When the link is recovered, the local port receives BFD packets from the peer port, and BFD notifies the Ethernet link aggregation module that the peer port is reachable. The local port is placed in Selected state again. This mechanism ensures that the local and peer ports of a static aggregate link have the same aggregation state.
- **BFD for dynamic aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. BFD clears the session and stops sending BFD packets. When the link is recovered and the local port is placed in Selected state again, the local port establishes a new session with the peer port. BFD notifies the Ethernet link aggregation module that the peer port is reachable. Because BFD provides fast failure detection, the local and peer systems of a dynamic aggregate link can negotiate the aggregation state of their member ports faster.

For more information about BFD, see *High Availability Configuration Guide*.

Configuration restrictions and guidelines

When you enable BFD for an aggregation group, follow these restrictions and guidelines:

- Make sure the source and destination IP addresses are consistent at the two ends of an aggregate link. For example, if you execute **link-aggregation bfd ipv4 source** 1.1.1.1 **destination** 2.2.2.2 on the local end, execute **link-aggregation bfd ipv4 source** 2.2.2.2 **destination** 1.1.1.1 on the peer end.
- The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode.

- As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.

Configuration procedure

To enable BFD for an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Enable BFD for the aggregation group.	**link-aggregation bfd ipv4 source** *ip-address* **destination** *ip-address*	By default, BFD is disabled for an aggregation group.

Shutting down an aggregate interface

Make sure no member port in an aggregation group is configured with the **loopback** command when you shut down the aggregate interface. Similarly, a port configured with the **loopback** command cannot be assigned to an aggregate interface already shut down. For more information about the **loopback** command, see *Layer 2—LAN Switching Command Reference*.

Shutting down or bringing up an aggregate interface affects the aggregation state and link state of ports in the corresponding aggregation group in the following ways:

- When an aggregate interface is shut down, all Selected ports in the corresponding aggregation group become unselected and their link state becomes down.
- When an aggregate interface is brought up, the aggregation state of ports in the corresponding aggregation group is recalculated.

To shut down an aggregate interface:

Step	Command
1. Enter system view.	**system-view**
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*
3. Shut down the aggregate interface.	**shutdown**

Restoring the default settings for an aggregate interface

You can return all configurations on an aggregate interface to default settings.

To restore the default settings for an aggregate interface:

Step	Command
1. Enter system view.	**system-view**
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*
3. Restore the default settings for the aggregate interface.	**default**

Configuring load sharing for link aggregation groups

Setting load sharing modes for link aggregation groups

You can set the global or group-specific load sharing mode. A link aggregation group preferentially uses the group-specific load sharing mode. If the group-specific load sharing mode is not available, the group uses the global load sharing mode.

Setting the global link-aggregation load sharing mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the global link-aggregation load sharing mode.	**link-aggregation global load-sharing mode** { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *	By default, the system automatically chooses the global link-aggregation load sharing mode according to the packet type.

Setting the group-specific load sharing mode

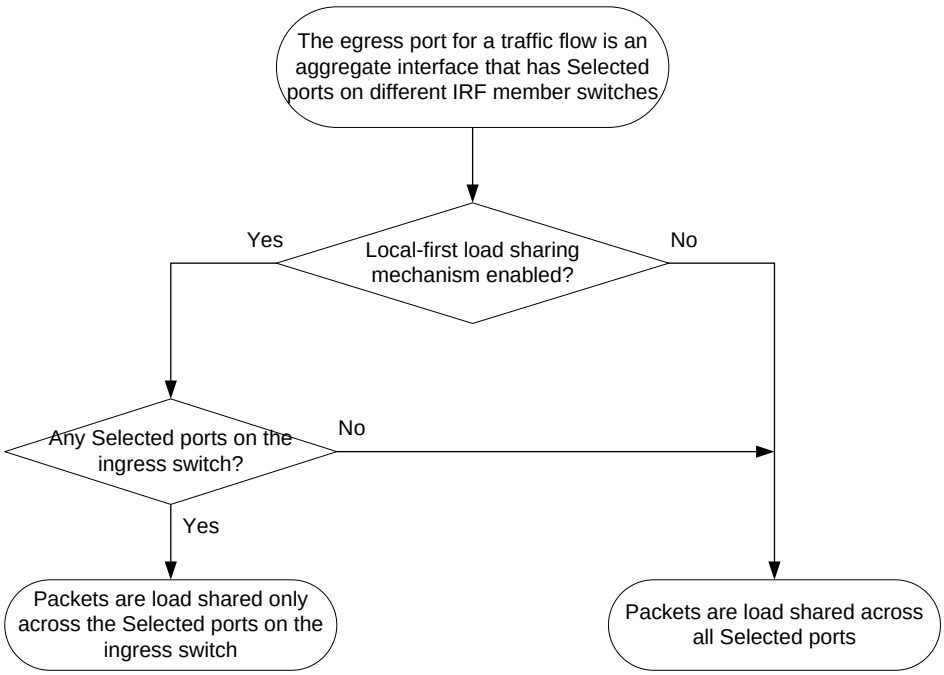
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Configure the load sharing mode for the aggregation group.	**link-aggregation load-sharing mode** { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *	The default settings are the same as the global load sharing mode.

Enabling local-first load sharing for link aggregation

Use local-first load sharing in a multidevice link aggregation scenario to distribute traffic preferentially across member ports on the ingress card or device.

When you aggregate ports on different member devices in an IRF fabric, you can use local-first load sharing to reduce traffic on IRF links, as shown in Figure 11. For more information about IRF, see *IRF Configuration Guide*.

Figure 11 Load sharing for multiswitch link aggregation in an IRF fabric



To enable local-first load sharing for link aggregation:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable local-first load sharing for link aggregation.	**link-aggregation load-sharing mode local-first**	By default, local-first load sharing for link aggregation is enabled.

Configuring per-flow load sharing algorithm settings for Ethernet link aggregation

Configure the per-flow load sharing algorithm and algorithm seed to optimize traffic distribution on aggregate links based on existing per-flow load sharing settings. You can set only the algorithm or the algorithm seed, or both. You can combine an algorithm with different algorithm seeds to obtain different effects.

This feature does not take effect on per-flow load sharing that uses the following traffic classification criteria:

- Source IP address.
- Destination IP address.
- Source MAC address.

- Destination MAC address.
- Source and destination IP addresses.
- Source and destination MAC addresses.

To configure per-flow load sharing algorithm settings for Ethernet link aggregation:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the load sharing algorithm.	**link-aggregation global load-sharing algorithm** *algorithm-number*	By default, algorithm 0 is used.
3. Configure the load sharing algorithm seed.	**link-aggregation global load-sharing seed** *seed-number*	By default, algorithm seed 0 is used.

Enabling link-aggregation traffic redirection

IMPORTANT:

In Release 1111, this feature is supported only in system view. In Release 1121 and later, this feature is supported in system view, Layer 2 aggregate interface view, and Layer 3 aggregate interface view.

Link-aggregation traffic redirection prevents traffic interruption.

When you shut down a Selected port in an aggregation group, this feature redirects traffic to other Selected ports.

When you restart an IRF member device that contains Selected ports, this feature redirects traffic to other IRF member devices.

You can enable link-aggregation traffic redirection globally or for an aggregation group. Global link-aggregation traffic redirection settings take effect on all aggregation groups. A link aggregation group preferentially uses the group-specific link-aggregation traffic redirection settings. If group-specific link-aggregation traffic redirection is not configured, the group uses the global link-aggregation traffic redirection settings.

Configuration restrictions and guidelines

When you enable ink-aggregation traffic redirection, follow these restrictions and guidelines:

- Link-aggregation traffic redirection applies only to dynamic link aggregation groups and takes effect on only known unicast packets.
- To prevent traffic interruption, enable link-aggregation traffic redirection on devices at both ends of the aggregate link.
- To prevent packet loss that might occur at a reboot, do not enable spanning tree together with link-aggregation traffic redirection.
- Link-aggregation traffic redirection does not operate correctly on an edge aggregate interface.
- As a best practice, enable link-aggregation traffic redirection on aggregate interfaces. If you enable this feature globally, communication with a third-party peer device might be affected if the peer is not compatible with this feature.

Configuration procedure

To enable link-aggregation traffic redirection globally:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable link-aggregation traffic redirection globally.	**link-aggregation lacp traffic-redirect-notification enable**	By default, link-aggregation traffic redirection is disabled globally.

To enable link-aggregation traffic redirection for an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Enable link-aggregation traffic redirection for the aggregation group.	**link-aggregation lacp traffic-redirect-notification enable**	By default, link-aggregation traffic redirection is disabled for an aggregation group.

Specifying link aggregation management VLANs and management port

IMPORTANT:

This feature is available in Release 1122P02 and later.

For an aggregation group to forward Layer 3 data traffic of some VLANs through a specific port, specify the VLANs as management VLANs and the port as a management port.

To specify link aggregation management VLANs and management port for an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify link aggregation management VLANs.	**link-aggregation management-vlan** *vlan-id-list*	By default, no link aggregation management VLANs are specified.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the port as a management port for its aggregation group.	**link-aggregation management-port**	By default, a port does not act as a management port in its aggregation group.

Displaying and maintaining Ethernet link aggregation

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information for an aggregate interface or multiple aggregate interfaces.	**display interface** [**bridge-aggregation** | **route-aggregation**] [**brief** [**down**]] **display interface** [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]] [**brief** [**description**]]
Display the local system ID.	**display lacp system-id**
Display the global or group-specific link-aggregation load sharing modes.	**display link-aggregation load-sharing mode** [**interface** [{ **bridge-aggregation** | **route-aggregation** } *interface-number*]]
Display detailed link aggregation information for link aggregation member ports.	**display link-aggregation member-port** [*interface-list*]
Display summary information about all aggregation groups.	**display link-aggregation summary**
Display detailed information about the specified aggregation groups.	**display link-aggregation verbose** [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]]
Clear LACP statistics for the specified link aggregation member ports.	**reset lacp statistics** [**interface** *interface-list*]
Clear statistics for the specified aggregate interfaces.	**reset counters interface** [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]]

Ethernet link aggregation configuration examples

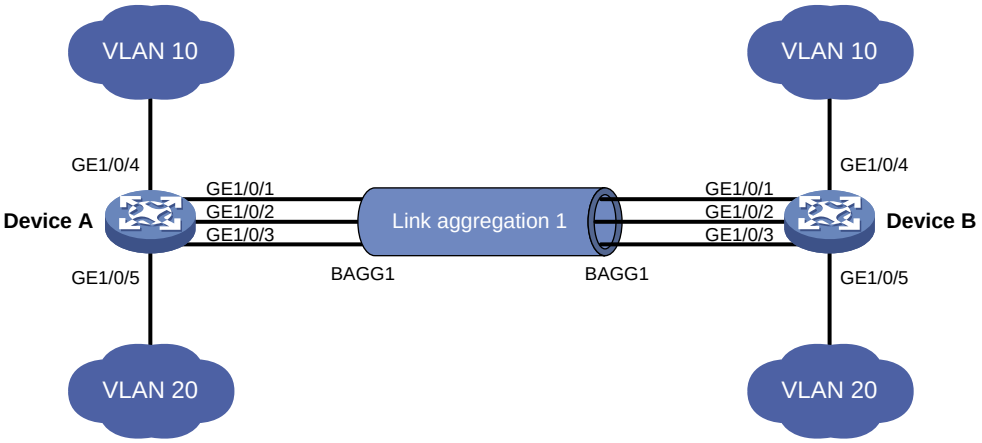
Layer 2 static aggregation configuration example

Network requirements

On the network shown in Figure 12, perform the following tasks:

- Configure a Layer 2 static aggregation group on both Device A and Device B.
- Enable VLAN 10 at one end of the aggregate link to communicate with VLAN 10 at the other end.
- Enable VLAN 20 at one end of the aggregate link to communicate with VLAN 20 at the other end.

Figure 12 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLAN 10, and assign port GigabitEthernet 1/0/4 to VLAN 10.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] port gigabitethernet 1/0/4
   [DeviceA-vlan10] quit
   ```

   # Create VLAN 20, and assign port GigabitEthernet 1/0/5 to VLAN 20.

   ```
   [DeviceA] vlan 20
   [DeviceA-vlan20] port gigabitethernet 1/0/5
   [DeviceA-vlan20] quit
   ```

   # Create Layer 2 aggregate interface Bridge-Aggregation 1.

   ```
   [DeviceA] interface bridge-aggregation 1
   [DeviceA-Bridge-Aggregation1] quit
   ```

   # Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to link aggregation group 1.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/2] quit
   [DeviceA] interface gigabitethernet 1/0/3
   [DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/3] quit
   ```

   # Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a trunk port and assign it to VLANs 10 and 20.

   ```
   [DeviceA] interface bridge-aggregation 1
   [DeviceA-Bridge-Aggregation1] port link-type trunk
   [DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
   [DeviceA-Bridge-Aggregation1] quit
   ```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port                Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1             S       32768    1
  GE1/0/2             S       32768    1
  GE1/0/3             S       32768    1
```

The output shows that:

- Link aggregation group 1 is a Layer 2 static aggregation group.
- The aggregation group contains three Selected ports.

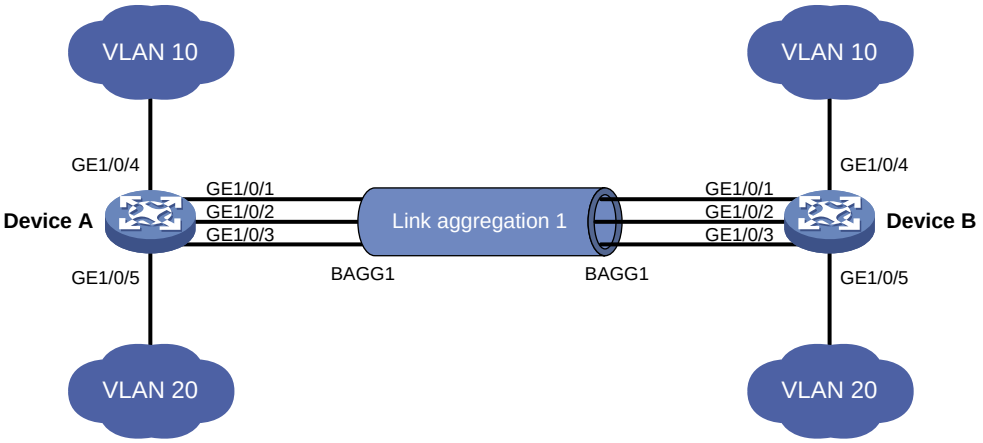
Layer 2 dynamic aggregation configuration example

Network requirements

On the network shown in Figure 13, perform the following tasks:

- Configure a Layer 2 dynamic aggregation group on both Device A and Device B.
- Enable VLAN 10 at one end of the aggregate link to communicate with VLAN 10 at the other end.
- Enable VLAN 20 at one end of the aggregate link to communicate with VLAN 20 at the other end.

Figure 13 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLAN 10, and assign the port GigabitEthernet 1/0/4 to VLAN 10.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 10
   ```

```
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

Create VLAN 20, and assign the port GigabitEthernet 1/0/5 to VLAN 20.

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 1, and set the link aggregation mode to dynamic.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to link aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a trunk port and assign it to VLANs 10 and 20.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
[DeviceA-Bridge-Aggregation1] quit
```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port               Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1            S       32768    1         {ACDEF}
  GE1/0/2            S       32768    1         {ACDEF}
  GE1/0/3            S       32768    1         {ACDEF}
Remote:
```

```
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          1       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2          2       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3          3       32768    1         0x8000, 000f-e267-57ad {ACDEF}
```

The output shows that:

- Link aggregation group 1 is a Layer 2 dynamic aggregation group.
- The aggregation group contains three Selected ports.

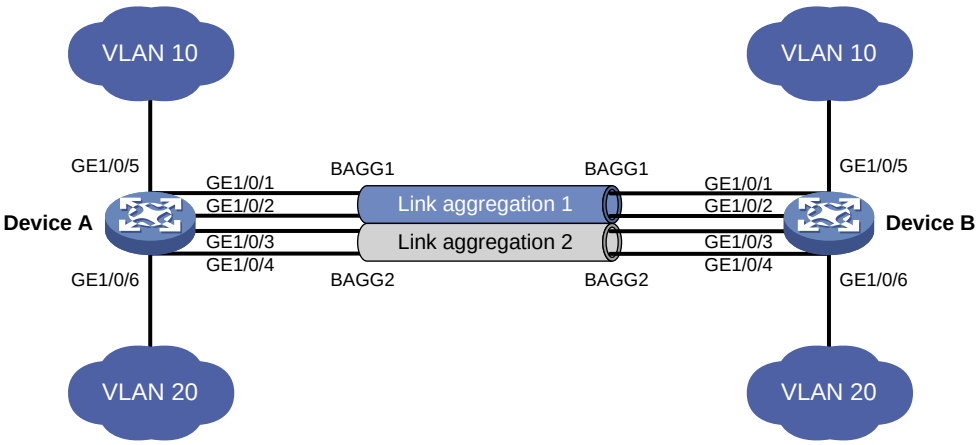
Layer 2 aggregation load sharing configuration example

Network requirements

On the network shown in Figure 14, perform the following tasks:

- Configure two Layer 2 static aggregation groups 1 and 2 on Device A and Device B, respectively.
- Enable VLAN 10 at one end of the aggregate link to communicate with VLAN 10 at the other end.
- Enable VLAN 20 at one end of the aggregate link to communicate with VLAN 20 at the other end.
- Configure link aggregation groups 1 and 2 to load share traffic across aggregation group member ports.
  - Configure link aggregation group 1 to load share packets based on source MAC addresses.
  - Configure link aggregation group 2 to load share packets based on destination MAC addresses.

Figure 14 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLAN 10, and assign the port GigabitEthernet 1/0/5 to VLAN 10.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] port gigabitethernet 1/0/5
   [DeviceA-vlan10] quit
   ```

   # Create VLAN 20, and assign the port GigabitEthernet 1/0/6 to VLAN 20.

   ```
   [DeviceA] vlan 20
   ```

```
[DeviceA-vlan20] port gigabitethernet 1/0/6
[DeviceA-vlan20] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
```

Configure Layer 2 aggregation group 1 to load share packets based on source MAC addresses.

```
[DeviceA-Bridge-Aggregation1] link-aggregation load-sharing mode source-mac
[DeviceA-Bridge-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to link aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a trunk port and assign it to VLAN 10.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10
[DeviceA-Bridge-Aggregation1] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 2.

```
[DeviceA] interface bridge-aggregation 2
```

Configure Layer 2 aggregation group 2 to load share packets based on destination MAC addresses.

```
[DeviceA-Bridge-Aggregation2] link-aggregation load-sharing mode destination-mac
[DeviceA-Bridge-Aggregation2] quit
```

Assign ports GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to link aggregation group 2.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 2 as a trunk port and assign it to VLAN 20.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] port link-type trunk
[DeviceA-Bridge-Aggregation2] port trunk permit vlan 20
[DeviceA-Bridge-Aggregation2] quit
```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
```

```
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port               Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1            S       32768    1
  GE1/0/2            S       32768    1

Aggregate Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
    Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/3            S       32768    2
  GE1/0/4            S       32768    2
```

The output shows that:

- Link aggregation groups 1 and 2 are both load-shared Layer 2 static aggregation groups.
- Each aggregation group contains two Selected ports.

Display all the group-specific load sharing modes on Device A.

```
[DeviceA] display link-aggregation load-sharing mode interface

Bridge-Aggregation1 Load-Sharing Mode:
source-mac address

Bridge-Aggregation2 Load-Sharing Mode:
destination-mac address
```

The output shows that:

- Link aggregation group 1 load shares packets based on source MAC addresses.
- Link aggregation group 2 load shares packets based on destination MAC addresses.

Layer 2 edge aggregate interface configuration example

Network requirements

As shown in Figure 15, a Layer 2 dynamic aggregation group is configured on the device. The server is not configured with dynamic link aggregation.

Configure an edge aggregate interface so that both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 can forward traffic to improve link reliability.

Figure 15 Network diagram

Configuration procedure

Create Layer 2 aggregate interface Bridge-Aggregation 1, and set the link aggregation mode to dynamic.

```
<Device> system-view
[Device] interface bridge-aggregation 1
[Device-Bridge-Aggregation1] link-aggregation mode dynamic
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an edge aggregate interface.

```
[Device-Bridge-Aggregation1] lacp edge-port
[Device-Bridge-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to link aggregation group 1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-aggregation group 1
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-aggregation group 1
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display detailed information about all aggregation groups on the device when the server is not configured with dynamic link aggregation.

```
[Device] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: NonS
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          I       32768    1         {AG}
  GE1/0/2          I       32768    1         {AG}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          0       32768    0         0x8000, 0000-0000-0000 {DEF}
  GE1/0/2          0       32768    0         0x8000, 0000-0000-0000 {DEF}
```

The output shows that GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in Individual state when they do not receive LACPDUs from the server. Both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 can forward traffic. When one port fails, its traffic is automatically switched to the other port.

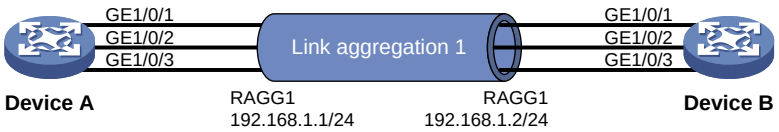
Layer 3 static aggregation configuration example

Network requirements

On the network shown in Figure 16, perform the following tasks:

- Configure a Layer 3 static aggregation group on both Device A and Device B.
- Configure IP addresses and subnet masks for the corresponding Layer 3 aggregate interfaces.

Figure 16 Network diagram



Configuration procedure

1. Configure Device A:

   # Create Layer 3 aggregate interface Route-Aggregation 1, and configure an IP address and subnet mask for the aggregate interface.

   ```
   <DeviceA> system-view
   [DeviceA] interface route-aggregation 1
   [DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
   [DeviceA-Route-Aggregation1] quit
   ```

   # Assign Layer 3 Ethernet interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/2] quit
   [DeviceA] interface gigabitethernet 1/0/3
   [DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/3] quit
   ```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port               Status  Priority Oper-Key
--------------------------------------------------------------------------------
```

```
GE1/0/1            S       32768    1
GE1/0/2            S       32768    1
GE1/0/3            S       32768    1
```

The output shows that link aggregation group 1 is a non-load-shared Layer 3 static aggregation group that contains three Selected ports.

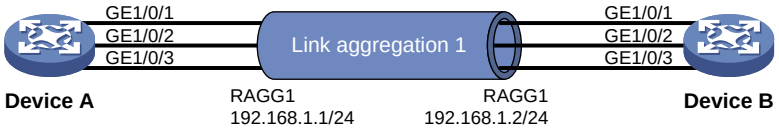
Layer 3 dynamic aggregation configuration example

Network requirements

On the network shown in Figure 17, perform the following tasks:

- Configure a Layer 3 dynamic aggregation group on both Device A and Device B.
- Configure IP addresses and subnet masks for the corresponding Layer 3 aggregate interfaces.

Figure 17 Network diagram



Configuration procedure

1. Configure Device A:

   # Create Layer 3 aggregate interface Route-Aggregation 1.

   ```
   <DeviceA> system-view
   [DeviceA] interface route-aggregation 1
   ```

   # Set the link aggregation mode to dynamic.

   ```
   [DeviceA-Route-Aggregation1] link-aggregation mode dynamic
   ```

   # Configure an IP address and subnet mask for Route-Aggregation 1.

   ```
   [DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
   [DeviceA-Route-Aggregation1] quit
   ```

   # Assign Layer 3 Ethernet interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/2] quit
   [DeviceA] interface gigabitethernet 1/0/3
   [DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
   [DeviceA-GigabitEthernet1/0/3] quit
   ```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
```

```
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1             S       32768    1         {ACDEF}
  GE1/0/2             S       32768    1         {ACDEF}
  GE1/0/3             S       32768    1         {ACDEF}
Remote:
  Actor             Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1           1       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2           2       32768    1         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3           3       32768    1         0x8000, 000f-e267-57ad {ACDEF}
```

The output shows that:

- Link aggregation group 1 is a non-load-shared Layer 3 dynamic aggregation group.
- The aggregation group contains three Selected ports.

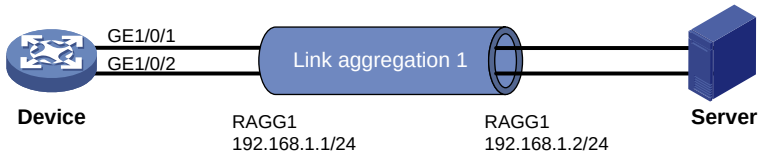
Layer 3 edge aggregate interface configuration example

Network requirements

As shown in Figure 18, a Layer 3 dynamic aggregation group is configured on the device. The server is not configured with dynamic link aggregation.

Configure an edge aggregate interface so that both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 can forward traffic to improve link reliability.

Figure 18 Network diagram



Configuration procedure

Create Layer 3 aggregate interface Route-Aggregation 1, and set the link aggregation mode to dynamic.

```
<Device> system-view
[Device] interface route-aggregation 1
[Device-Route-Aggregation1] link-aggregation mode dynamic
```

Configure an IP address and subnet mask for Layer 3 aggregate interface Route-Aggregation 1.

```
[Device-Route-Aggregation1] ip address 192.168.1.1 24
```

Configure Layer 3 aggregate interface Route-Aggregation 1 as an edge aggregate interface.

```
[Device-Route-Aggregation1] lacp edge-port
```

```
[Device-Route-Aggregation1] quit
```

Assign Layer 3 Ethernet interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-aggregation group 1
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-aggregation group 1
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display detailed information about all aggregation groups on the device when the server is not configured with dynamic link aggregation.

```
[Device] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: NonS
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          I       32768    1         {AG}
  GE1/0/2          I       32768    1         {AG}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          0       32768    0         0x8000, 0000-0000-0000 {DEF}
  GE1/0/2          0       32768    0         0x8000, 0000-0000-0000 {DEF}
```

The output shows that GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in Individual state when they do not receive LACPDUs from the server. Both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 can forward traffic. When one port fails, its traffic is automatically switched to the other port.

Configuring port isolation

The port isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs.

Ports in an isolation group cannot communicate with each other. However, they can communicate with ports outside the isolation group.

Assigning a port to an isolation group

The device supports multiple isolation groups, which can be configured manually. The number of ports assigned to an isolation group is not limited.

To assign a port to an isolation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an isolation group.	**port-isolate group** *group-number*	By default, no isolation group exists.
3. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	• The configuration in Layer 2 Ethernet interface view applies only to the interface. • The configuration in Layer 2 aggregate interface view applies to the Layer 2 aggregate interface and its aggregation member ports. If the device fails to apply the configuration to the aggregate interface, it does not assign any aggregation member port to the isolation group. If the failure occurs on an aggregation member port, the device skips the port and continues to assign other aggregation member ports to the isolation group.
4. Assign the port to the specified isolation group.	**port-isolate enable group** *group-number*	By default, the port is not in any isolation group. You can assign a port to at most one isolation group. If you execute the **port-isolate enable group** command multiple times, the most recent configuration takes effect.

Displaying and maintaining port isolation

Execute **display** commands in any view.

Task	Command
Display isolation group information.	**display port-isolate group** [*group-number*]

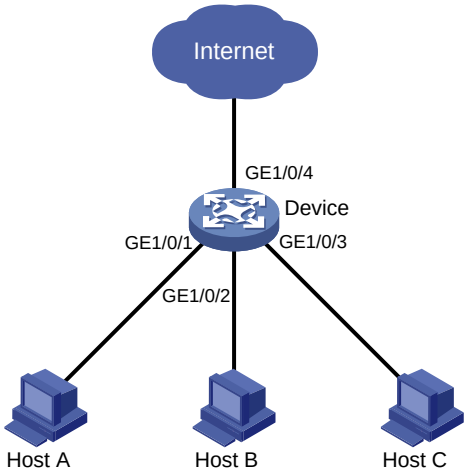
Port isolation configuration example

Network requirements

As shown in Figure 19, configure port isolation on the device to meet the following requirements:

- The hosts can access the Internet.
- The hosts cannot communicate with each other at Layer 2.

Figure 19 Network diagram



Configuration procedure

Create isolation group 2.

```
<Device> system-view
[Device] port-isolate group 2
```

Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to isolation group 2.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable group 2
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable group 2
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable group 2
```

Verifying the configuration

Display information about isolation group 2.

```
[Device] display port-isolate group 2
 Port isolation group information:
 Group ID: 2
 Group members:
    GigabitEthernet1/0/1
```

```
GigabitEthernet1/0/2
GigabitEthernet1/0/3
```

The output shows that interfaces GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are assigned to isolation group 2. As a result, Host A, Host B, and Host C are isolated from each other at layer 2.

Configuring spanning tree protocols

Spanning tree protocols eliminate loops in a physical link-redundant network by selectively blocking redundant links and putting them in a standby state.

The recent versions of STP include the Rapid Spanning Tree Protocol (RSTP), the Per-VLAN Spanning Tree (PVST), and the Multiple Spanning Tree Protocol (MSTP).

STP

STP was developed based on the 802.1d standard of IEEE to eliminate loops at the data link layer in a LAN. Networks often have redundant links as backups in case of failures, but loops are a very serious problem. Devices running STP detect loops in the network by exchanging information with one another. They eliminate loops by selectively blocking certain ports to prune the loop structure into a loop-free tree structure. This avoids proliferation and infinite cycling of packets that would occur in a loop network.

In a narrow sense, STP refers to IEEE 802.1d STP. In a broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

STP protocol packets

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets. This chapter uses BPDUs to represent all types of spanning tree protocol packets.

STP-enabled network devices exchange BPDUs to establish a spanning tree. BPDUs contain sufficient information for the network devices to complete spanning tree calculation.

STP uses the following types of BPDUs:

- **Configuration BPDUs**—Used by the network devices to calculate a spanning tree and maintain the spanning tree topology.
- **Topology change notification (TCN) BPDUs**—Notify network devices of network topology changes.

Configuration BPDUs contain sufficient information for the network devices to complete spanning tree calculation. Important fields in a configuration BPDU include the following:

- **Root bridge ID**—Consisting of the priority and MAC address of the root bridge.
- **Root path cost**—Cost of the path to the root bridge denoted by the root identifier from the transmitting bridge.
- **Designated bridge ID**—Consisting of the priority and MAC address of the designated bridge.
- **Designated port ID**—Consisting of the priority and global port number of the designated port.
- **Message age**—Age of the configuration BPDU while it propagates in the network.
- **Max age**—Maximum age of the configuration BPDU stored on the switch.
- **Hello time**—Configuration BPDU transmission interval.
- **Forward delay**—Delay that STP bridges use to transit port state.

Basic concepts in STP

Root bridge

A tree network must have a root bridge. The entire network contains only one root bridge, and all the other bridges in the network are called leaf nodes. The root bridge is not permanent, but can change with changes of the network topology.

Upon initialization of a network, each device generates and periodically sends configuration BPDUs, with itself as the root bridge. After network convergence, only the root bridge generates and periodically sends configuration BPDUs. The other devices only forward the BPDUs.

Root port

On a non-root bridge, the port nearest to the root bridge is the root port. The root port communicates with the root bridge. Each non-root bridge has only one root port. The root bridge has no root port.

Designated bridge and designated port

Classification	Designated bridge	Designated port
For a device	Device directly connected with the local device and responsible for forwarding BPDUs to the local device.	Port through which the designated bridge forwards BPDUs to this device.
For a LAN	Device responsible for forwarding BPDUs to this LAN segment.	Port through which the designated bridge forwards BPDUs to this LAN segment.

As shown in Figure 20, Device B and Device C are directly connected to a LAN.

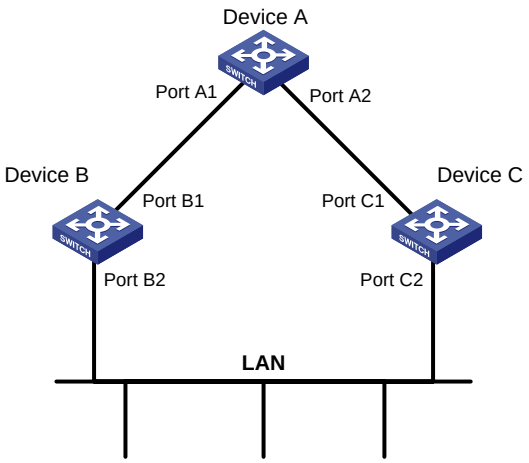
If Device A forwards BPDUs to Device B through port A1, the designated bridge and designated port are as follows:

- The designated bridge for Device B is Device A.
- The designated port of Device B is port A1 on Device A.

If Device B forwards BPDUs to the LAN, the designated bridge and designated port are as follows:

- The designated bridge for the LAN is Device B.
- The designated port for the LAN is port B2 on Device B.

Figure 20 Designated bridges and designated ports



Path cost

Path cost is a reference value used for link selection in STP. To prune the network into a loop-free tree, STP calculates path costs to select the most robust links and block redundant links that are less robust.

Calculation process of the STP algorithm

The spanning tree calculation process described in the following sections is an example of a simplified process.

Calculation process

The STP algorithm uses the following calculation process:

1. Initialize the network.

   Upon initialization of a device, each port generates a BPDU with the following contents:

   - The port as the designated port.
   - The device as the root bridge.
   - 0 as the root path cost.
   - The device ID as the designated bridge ID.

2. Select the root bridge.

   Initially, each STP-enabled device on the network assumes itself to be the root bridge, with its own device ID as the root bridge ID. By exchanging configuration BPDUs, the devices compare their root bridge IDs to elect the device with the smallest root bridge ID as the root bridge.

3. Root port and designated ports selection on the non-root bridges.

Step	Description
1	A non-root–bridge device regards the port on which it received the optimum configuration BPDU as the root port. Table 5 describes how the optimum configuration BPDU is selected.
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the other ports. • The root bridge ID is replaced with that of the configuration BPDU of the root port. • The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost of the root port. • The designated bridge ID is replaced with the ID of this device. • The designated port ID is replaced with the ID of this port.

3	The device compares the calculated configuration BPDU with the configuration BPDU on the port whose port role will be determined, and acts depending on the result of the comparison:
	• If the calculated configuration BPDU is superior, the device performs the following tasks:
	  ○ Considers this port as the designated port.
	  ○ Replaces the configuration BPDU on the port with the calculated configuration BPDU.
	  ○ Periodically sends the calculated configuration BPDU.
	• If the configuration BPDU on the port is superior, the device blocks this port without updating its configuration BPDU. The blocked port can receive BPDUs, but cannot send BPDUs or forward data traffic.

When the network topology is stable, only the root port and designated ports forward user traffic. Other ports are all in the blocked state to receive BPDUs but not to forward BPDUs or user traffic.

Table 5 Selecting the optimum configuration BPDU

Step	Actions
1	Upon receiving a configuration BPDU on a port, the device compares the priority of the received configuration BPDU with that of the configuration BPDU generated by the port. • If the former priority is lower, the device discards the received configuration BPDU and keeps the configuration BPDU the port generated. • If the former priority is higher, the device replaces the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum

	configuration BPDU.

The following are the principles of configuration BPDU comparison:

a. The configuration BPDU with the lowest root bridge ID has the highest priority.

b. If configuration BPDUs have the same root bridge ID, their root path costs are compared. For example, the root path cost in a configuration BPDU plus the path cost of a receiving port is S. The configuration BPDU with the smallest S value has the highest priority.

c. If all configuration BPDUs have the same root bridge ID and S value, the following attributes are compared in sequence:

- Designated bridge IDs.
- Designated port IDs.
- IDs of the receiving ports.

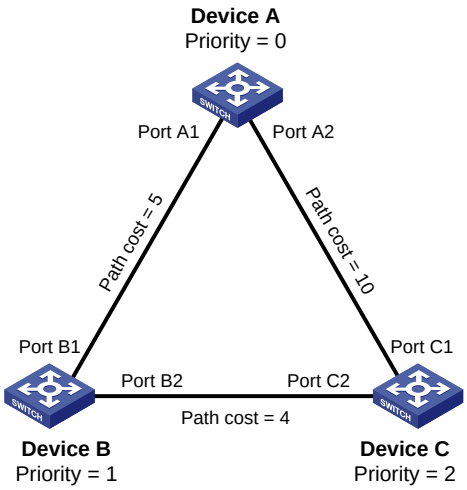
The configuration BPDU that contains a smaller designated bridge ID, designated port ID, or receiving port ID is selected.

A tree-shape topology forms when the root bridge, root ports, and designated ports are selected.

Example of STP calculation

Figure 21 provides an example showing how the STP algorithm works.

Figure 21 The STP algorithm



As shown in Figure 21, the priority values of Device A, Device B, and Device C are 0, 1, and 2, respectively. The path costs of links among the three devices are 5, 10, and 4.

1. Device state initialization.

In Table 6, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

Table 6 Initial state of each device

Device	Port name	Configuration BPDU on the port
Device A	Port A1	{0, 0, 0, Port A1}
	Port A2	{0, 0, 0, Port A2}
Device B	Port B1	{1, 0, 1, Port B1}
	Port B2	{1, 0, 1, Port B2}

Device C	Port C1	{2, 0, 2, Port C1}
	Port C2	{2, 0, 2, Port C2}

2. Configuration BPDUs comparison on each device.

   In Table 7, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

   Table 7 Comparison process and result on each device

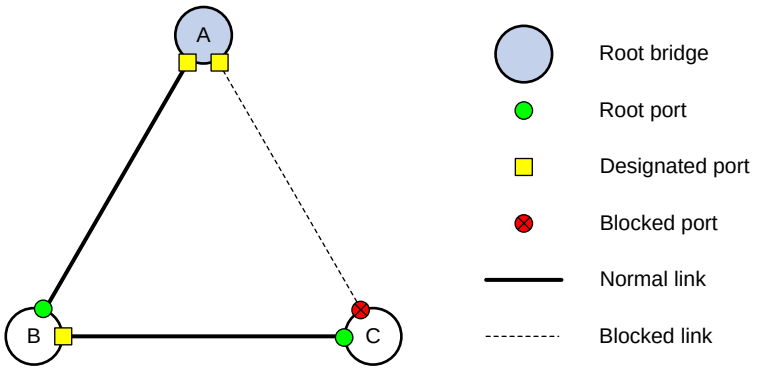
Device	Comparison process	Configuration BPDU on ports after comparison
Device A	Port A1 performs the following tasks: **1.** Receives the configuration BPDU of Port B1 {1, 0, 1, Port B1}. **2.** Determines that its existing configuration BPDU {0, 0, 0, Port A1} is superior to the received configuration BPDU. **3.** Discards the received one. Port A2 performs the following tasks: **1.** Receives the configuration BPDU of Port C1 {2, 0, 2, Port C1}. **2.** Determines that its existing configuration BPDU {0, 0, 0, Port A2} is superior to the received configuration BPDU. **3.** Discards the received one. Device A determines that it is both the root bridge and designated bridge in the configuration BPDUs of all its ports. It considers itself as the root bridge. It does not change the configuration BPDU of any port and starts to periodically send configuration BPDUs.	• Port A1: {0, 0, 0, Port A1} • Port A2: {0, 0, 0, Port A2}
Device B	Port B1 performs the following tasks: **1.** Receives the configuration BPDU of Port A1 {0, 0, 0, Port A1}. **2.** Determines that the received configuration BPDU is superior to its existing configuration BPDU {1, 0, 1, Port B1}. **3.** Updates its configuration BPDU. Port B2 performs the following tasks: **1.** Receives the configuration BPDU of Port C2 {2, 0, 2, Port C2}. **2.** Determines that its existing configuration BPDU {1, 0, 1, Port B2} is superior to the received configuration BPDU. **3.** Discards the received BPDU.	• Port B1: {0, 0, 0, Port A1} • Port B2: {1, 0, 1, Port B2}
	Device B performs the following tasks: **1.** Compares the configuration BPDUs of all its ports. **2.** Decides that the configuration BPDU of Port B1 is the optimum. **3.** Selects Port B1 as the root port with the configuration BPDU unchanged. Based on the configuration BPDU and path cost of the root port, Device B calculates a designated port configuration BPDU for Port B2 {0, 5, 1, Port B2}. Device B compares it with the existing configuration BPDU of Port B2 {1, 0, 1, Port B2}. Device B determines that the calculated one is superior, and determines that Port B2 is the designated port. It replaces the configuration BPDU on Port B2 with the calculated one, and periodically sends the calculated configuration BPDU.	• Root port (Port B1): {0, 0, 0, Port A1} • Designated port (Port B2): {0, 5, 1, Port B2}

Device C	Port C1 performs the following tasks: **1.** Receives the configuration BPDU of Port A2 {0, 0, 0, Port A2}. **2.** Determines that the received configuration BPDU is superior to its existing configuration BPDU {2, 0, 2, Port C1}. **3.** Updates its configuration BPDU. Port C2 performs the following tasks: **1.** Receives the original configuration BPDU of Port B2 {1, 0, 1, Port B2}. **2.** Determines that the received configuration BPDU is superior to the existing configuration BPDU {2, 0, 2, Port C2}. **3.** Updates its configuration BPDU.	• Port C1: {0, 0, 0, Port A2} • Port C2: {1, 0, 1, Port B2}
	Device C performs the following tasks: **1.** Compares the configuration BPDUs of all its ports. **2.** Decides that the configuration BPDU of Port C1 is the optimum. **3.** Selects Port C1 as the root port with the configuration BPDU unchanged. Based on the configuration BPDU and path cost of the root port, Device C calculates the configuration BPDU of Port C2 {0, 10, 2, Port C2}. Device C compares it with the existing configuration BPDU of Port C2 {1, 0, 1, Port B2}. Device C determines that the calculated configuration BPDU is superior to the existing one, selects Port C2 as the designated port, and replaces the configuration BPDU of Port C2 with the calculated one.	• Root port (Port C1): {0, 0, 0, Port A2} • Designated port (Port C2): {0, 10, 2, Port C2}
	Port C2 performs the following tasks: **1.** Receives the updated configuration BPDU of Port B2 {0, 5, 1, Port B2}. **2.** Determines that the received configuration BPDU is superior to its existing configuration BPDU {0, 10, 2, Port C2}. **3.** Updates its configuration BPDU. Port C1 performs the following tasks: **1.** Receives a periodic configuration BPDU {0, 0, 0, Port A2} from Port A2. **2.** Determines that it is the same as the existing configuration BPDU. **3.** Discards the received BPDU.	• Port C1: {0, 0, 0, Port A2} • Port C2: {0, 5, 1, Port B2}
	Device C determines that the root path cost of Port C1 (10) (root path cost of the received configuration BPDU (0) plus path cost of Port C1 (10)) is larger than that of Port C2 (9) (root path cost of the received configuration BPDU (5) plus path cost of Port C2 (4)). Device C determines that the configuration BPDU of Port C2 is the optimum, and selects Port C2 as the root port with the configuration BPDU unchanged. Based on the configuration BPDU and path cost of the root port, Device C performs the following tasks: **1.** Calculates a designated port configuration BPDU for Port C1 {0, 9, 2, Port C1}. **2.** Compares it with the existing configuration BPDU of Port C1 {0, 0, 0, Port A2}. **3.** Determines that the existing configuration BPDU is superior to the calculated one and blocks Port C1 with the configuration BPDU unchanged.	• Blocked port (Port C1): {0, 0, 0, Port A2} • Root port (Port C2): {0, 5, 1, Port B2}

	Port C1 does not forward data until a new event triggers a spanning tree calculation process: for example, the link between Device B and Device C is down.	

After the comparison processes described in Table 7, a spanning tree with Device A as the root bridge is established, as shown in Figure 22.

Figure 22 The final calculated spanning tree



The configuration BPDU forwarding mechanism of STP

The configuration BPDUs of STP are forwarded according to these guidelines:

- Upon network initiation, every device regards itself as the root bridge and generates configuration BPDUs with itself as the root. Then it sends the configuration BPDUs at a regular hello interval.
- If the root port received a configuration BPDU superior to the configuration BPDU of the port, the device performs the following tasks:
  - Increases the message age carried in the configuration BPDU.
  - Starts a timer to time the configuration BPDU.
  - Sends this configuration BPDU through the designated port.
- If a designated port receives a configuration BPDU with a lower priority than its configuration BPDU, the port immediately responds with its configuration BPDU.
- If a path fails, the root port on this path no longer receives new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. The device generates a configuration BPDU with itself as the root and sends the BPDUs and TCN BPDUs. This triggers a new spanning tree calculation process to establish a new path to restore the network connectivity.

However, the newly calculated configuration BPDU cannot be propagated throughout the network immediately. As a result, the old root ports and designated ports that have not detected the topology change continue forwarding data along the old path. If the new root ports and designated ports begin to forward data as soon as they are elected, a temporary loop might occur.

STP timers

The most important timing parameters in STP calculation are forward delay, hello time, and max age.

- Forward delay

  Forward delay is the delay time for port state transition.

  A path failure can cause spanning tree recalculation to adapt the spanning tree structure to the change. However, the resulting new configuration BPDU cannot propagate throughout the network immediately. If the newly elected root ports and designated ports start to forward data immediately, a temporary loop will likely occur.

The newly elected root ports or designated ports require twice the forward delay time before they transit to the forwarding state. This allows the new configuration BPDU to propagate throughout the network.

- Hello time

  The device sends hello packets at the hello time interval to the neighboring devices to make sure the paths are fault-free.

- Max age

  The device uses the max age to determine whether a stored configuration BPDU has expired and discards it if the max age is exceeded.

RSTP

RSTP achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much faster than STP.

A newly elected RSTP root port rapidly enters the forwarding state when the following conditions exist:

- The old root port on the device has stopped forwarding data.
- The upstream designated port has started forwarding data.

A newly elected RSTP designated port rapidly enters the forwarding state if it is an edge port or it connects to a point-to-point link.

- A port that directly connects to a user terminal can be configured as an edge port. Edge ports directly enter the forwarding state.
- When a designated port connects to a point-to-point link, it enters the forwarding state immediately after the device receives a handshake response from the directly connected device.

PVST

In an STP- or RSTP-enabled LAN, all bridges share one spanning tree. Traffic from all VLANs is forwarded along the spanning tree, and ports cannot be blocked on a per-VLAN basis to prune loops.

PVST allows every VLAN to have its own spanning tree, which increases utilization of links and bandwidth. Because each VLAN runs STP or RSTP independently, a spanning tree only serves its VLAN.

A PVST-enabled HPE device can communicate with a third-party device that is running Rapid PVST or PVST. The PVST-enabled HPE device supports fast network convergence like RSTP when connected to PVST-enabled HPE devices or third-party devices enabled with Rapid PVST.

A port's link type determines the type of BPDUs the port sends.

- An access port sends STP BPDUs.
- A trunk or hybrid port sends STP BPDUs in VLAN 1 and sends PVST BPDUs in other VLANs.

MSTP

MSTP overcomes the following STP, RSTP, and PVST limitations:

- **STP limitations**—STP does not support rapid state transition of ports. A newly elected port must wait twice the forward delay time before it transits to the forwarding state.
- **RSTP limitations**—Although RSTP enables faster network convergence than STP, RSTP fails to provide load balancing among VLANs. As with STP, all RSTP bridges in a LAN share one spanning tree and forward packets from all VLANs along this spanning tree.

- **PVST limitations**—Because each VLAN has its spanning tree, the amount of PVST BPDUs is proportional to the number of VLANs on a trunk or hybrid port. When the trunk or hybrid port permits too many VLANs, both resources and calculations for maintaining the VLAN spanning trees increase dramatically. If a status change occurs on the trunk or hybrid port that permits multiple VLANs, the device CPU will be overburdened with recalculating the affected spanning trees. As a result, network performance is degraded.

MSTP features

Developed based on IEEE 802.1s, MSTP overcomes the limitations of STP, RSTP, and PVST. In addition to supporting rapid network convergence, it allows data flows of different VLANs to be forwarded along separate paths. This provides a better load sharing mechanism for redundant links.

MSTP provides the following features:

- MSTP divides a switched network into multiple regions, each of which contains multiple spanning trees that are independent of one another.
- MSTP supports mapping VLANs to spanning tree instances by means of a VLAN-to-instance mapping table. MSTP can reduce communication overheads and resource usage by mapping multiple VLANs to one instance.
- MSTP prunes a loop network into a loop-free tree, which avoids proliferation and endless cycling of packets in a loop network. In addition, it supports load balancing of VLAN data by providing multiple redundant paths for data forwarding.
- MSTP is compatible with STP and RSTP, and partially compatible with PVST.

MSTP basic concepts

Figure 23 shows a switched network that comprises four MST regions, each MST region comprising four MSTP devices. Figure 24 shows the networking topology of MST region 3.

Figure 23 Basic concepts in MSTP

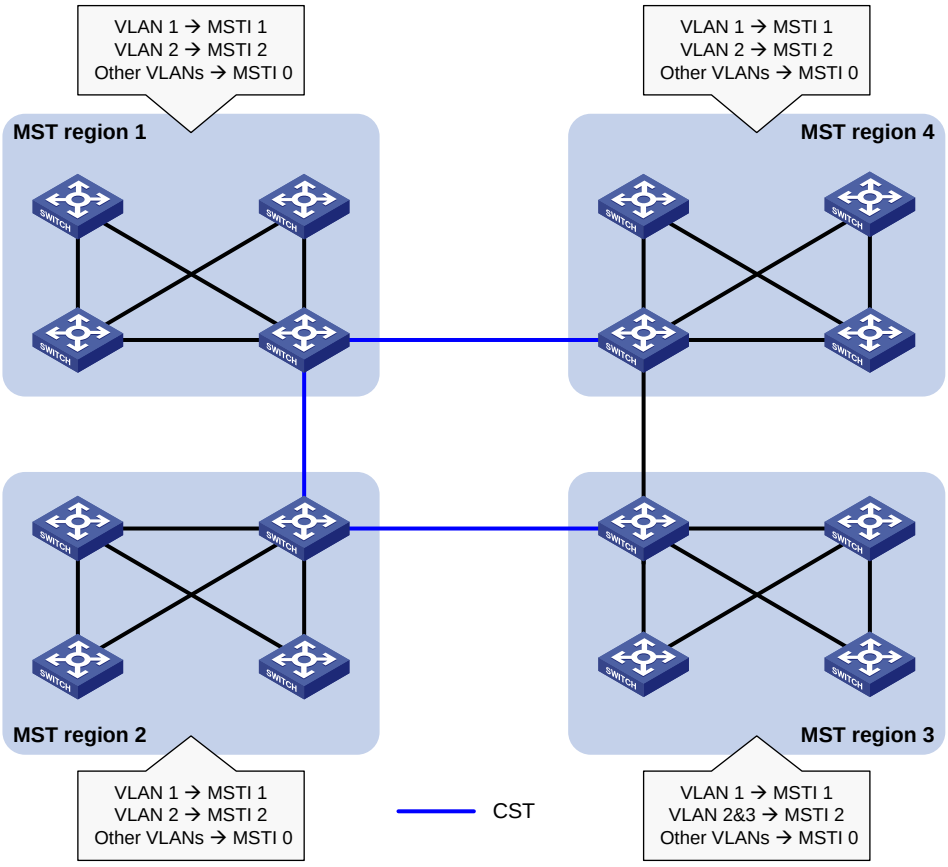
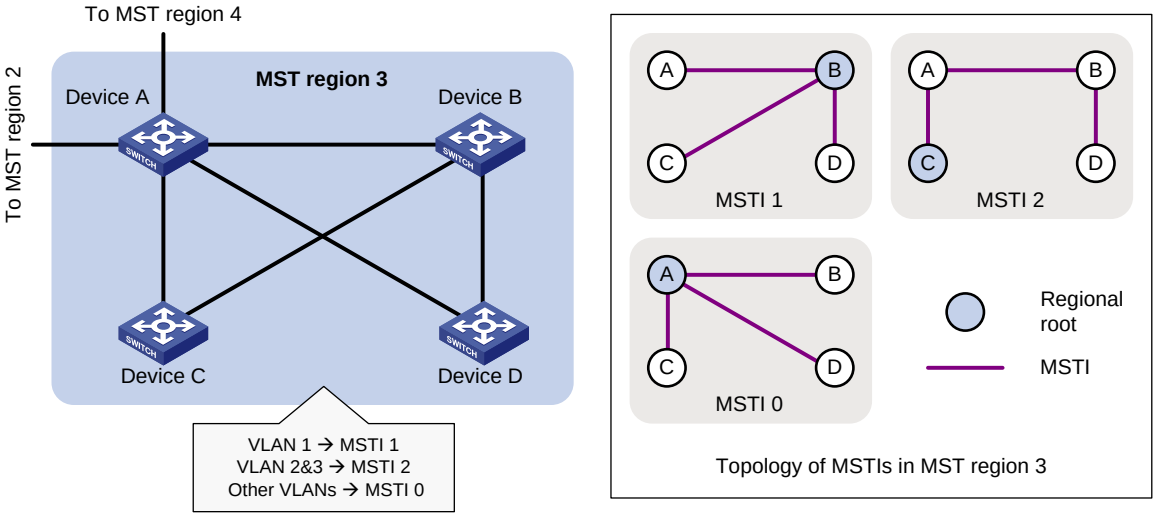


Figure 24 Network diagram and topology of MST region 3



MST region

A multiple spanning tree region (MST region) consists of multiple devices in a switched network and the network segments among them. All these devices have the following characteristics:

- A spanning tree protocol enabled
- Same region name
- Same VLAN-to-instance mapping configuration

- Same MSTP revision level
- Physically linked together

Multiple MST regions can exist in a switched network. You can assign multiple devices to the same MST region as shown in Figure 23.

- The switched network comprises four MST regions, MST region 1 through MST region 4.
- All devices in each MST region have the same MST region configuration.

MSTI

MSTP can generate multiple independent spanning trees in an MST region, and each spanning tree is mapped to the specific VLANs. Each spanning tree is referred to as a multiple spanning tree instance (MSTI).

In Figure 24, MST region 3 comprises three MSTIs, MSTI 1, MSTI 2, and MSTI 0.

VLAN-to-instance mapping table

As an attribute of an MST region, the VLAN-to-instance mapping table describes the mapping relationships between VLANs and MSTIs.

In Figure 24, the VLAN-to-instance mapping table of MST region 3 is as follows:

- VLAN 1 to MSTI 1.
- VLAN 2 and VLAN 3 to MSTI 2.
- Other VLANs to MSTI 0.

MSTP achieves load balancing by means of the VLAN-to-instance mapping table.

CST

The common spanning tree (CST) is a single spanning tree that connects all MST regions in a switched network. If you regard each MST region as a device, the CST is a spanning tree calculated by these devices through STP or RSTP.

The blue lines in Figure 23 represent the CST.

IST

An internal spanning tree (IST) is a spanning tree that runs in an MST region. It is also called MSTI 0, a special MSTI to which all VLANs are mapped by default.

In Figure 23, MSTI 0 is the IST in MST region 3.

CIST

The common and internal spanning tree (CIST) is a single spanning tree that connects all devices in a switched network. It consists of the ISTs in all MST regions and the CST.

In Figure 23, the ISTs (MSTI 0) in all MST regions plus the inter-region CST constitute the CIST of the entire network.

Regional root

The root bridge of the IST or an MSTI within an MST region is the regional root of the IST or MSTI. Based on the topology, different spanning trees in an MST region might have different regional roots, as shown in MST region 3 in Figure 24:

- The regional root of MSTI 1 is Device B.
- The regional root of MSTI 2 is Device C.
- The regional root of MSTI 0 (also known as the IST) is Device A.

Common root bridge

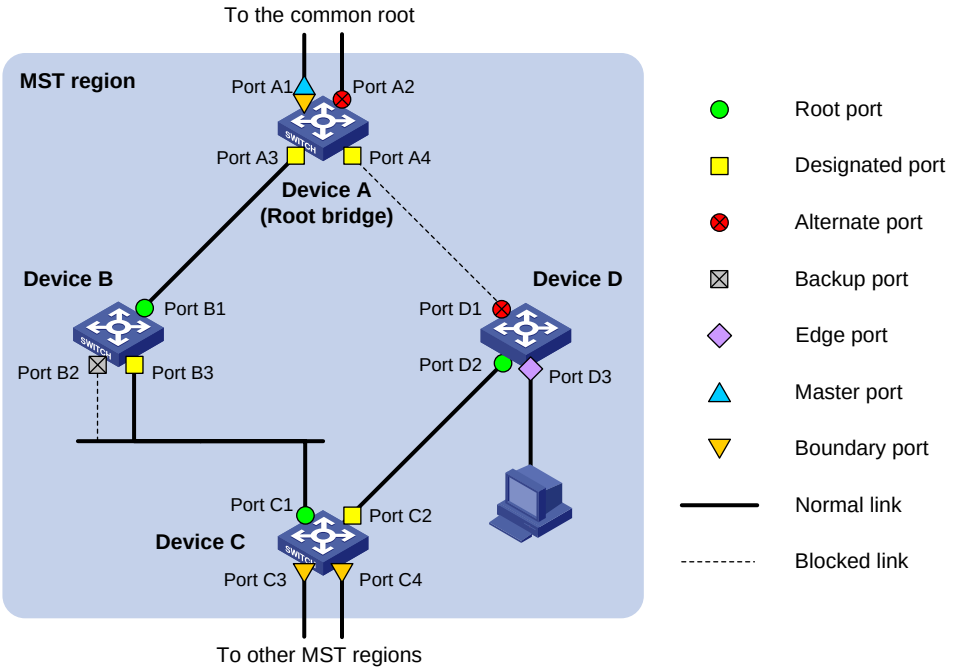
The common root bridge is the root bridge of the CIST.

In Figure 23, the common root bridge is a device in MST region 1.

Port roles

A port can play different roles in different MSTIs. As shown in Figure 25, an MST region comprises Device A, Device B, Device C, and Device D. Port A1 and port A2 of Device A connect to the common root bridge. Port B2 and Port B3 of Device B form a loop. Port C3 and Port C4 of Device C connect to other MST regions. Port D3 of Device D directly connects to a host.

Figure 25 Port roles



MSTP calculation involves the following port roles:

- **Root port**—Forwards data for a non-root bridge to the root bridge. The root bridge does not have any root port.
- **Designated port**—Forwards data to the downstream network segment or device.
- **Alternate port**—Acts as the backup port for a root port or master port. When the root port or master port is blocked, the alternate port takes over.
- **Backup port**—Acts as the backup port of a designated port. When the designated port is invalid, the backup port becomes the new designated port. A loop occurs when two ports of the same spanning tree device are connected, so the device blocks one of the ports. The blocked port acts as the backup.
- **Edge port**—Does not connect to any network device or network segment, but directly connects to a user host.
- **Master port**—Acts as a port on the shortest path from the local MST region to the common root bridge. The master port is not always located on the regional root. It is a root port on the IST or CIST and still a master port on the other MSTIs.
- **Boundary port**—Connects an MST region to another MST region or to an STP/RSTP-running device. In MSTP calculation, a boundary port's role on an MSTI is consistent with its role on the CIST. However, that is not true with master ports. A master port on MSTIs is a root port on the CIST.

Port states

In MSTP, a port can be in one of the following states:

- **Forwarding**—The port receives and sends BPDUs, learns MAC addresses, and forwards user traffic.

- **Learning**—The port receives and sends BPDUs, learns MAC addresses, but does not forward user traffic. Learning is an intermediate port state.
- **Discarding**—The port receives and sends BPDUs, but does not learn MAC addresses or forward user traffic.

NOTE:

When in different MSTIs, a port can be in different states.

A port state is not exclusively associated with a port role. Table 8 lists the port states that each port role supports. (A check mark [√] indicates that the port supports this state, while a dash [—] indicates that the port does not support this state.)

Table 8 Port states that different port roles support

Port role (right) Port state (below)	Root port/master port	Designated port	Alternate port	Backup port
Forwarding	√	√	—	—
Learning	√	√	—	—
Discarding	√	√	√	√

How MSTP works

MSTP divides an entire Layer 2 network into multiple MST regions, which are connected by a calculated CST. Inside an MST region, multiple spanning trees, called MSTIs, are calculated. Among these MSTIs, MSTI 0 is the IST.

Like STP, MSTP uses configuration BPDUs to calculate spanning trees. An important difference is that an MSTP BPDU carries the MSTP configuration of the bridge from which the BPDU is sent.

CIST calculation

During the CIST calculation, the following process takes place:

- The device with the highest priority is elected as the root bridge of the CIST.
- MSTP generates an IST within each MST region through calculation.
- MSTP regards each MST region as a single device and generates a CST among these MST regions through calculation.

The CST and ISTs constitute the CIST of the entire network.

MSTI calculation

Within an MST region, MSTP generates different MSTIs for different VLANs based on the VLAN-to-instance mappings. For each spanning tree, MSTP performs a separate calculation process similar to spanning tree calculation in STP. For more information, see "Calculation process of the STP algorithm."

In MSTP, a VLAN packet is forwarded along the following paths:

- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

MSTP implementation on devices

MSTP is compatible with STP and RSTP. Devices that are running MSTP and that are used for spanning tree calculation can identify STP and RSTP protocol packets.

In addition to basic MSTP functions, the following functions are provided for ease of management:

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU guard
- Port role restriction
- TC-BPDU transmission restriction

Protocols and standards

MSTP is documented in the following 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*
- IEEE 802.1Q-REV/D1.3, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks —Clause 13: Spanning tree Protocols*

Spanning tree configuration task lists

Before configuring a spanning tree, complete the following tasks:

- Determine the spanning tree protocol to be used (STP, RSTP, PVST, or MSTP).
- Plan the device roles (the root bridge or leaf node).

When you configure spanning tree protocols, follow these restrictions and guidelines:

- If both MVRP and a spanning tree protocol are enabled on a device, MVRP packets are forwarded along MSTIs. To advertise a specific VLAN within the network through MVRP, make sure this VLAN is mapped to an MSTI when you configure the VLAN-to-instance mapping table. For more information about MVRP, see "Configuring MVRP."
- The spanning tree configurations are mutually exclusive with service loopback and Smart Link.
- Configurations made in system view take effect globally. Configurations made in Ethernet interface view or WLAN mesh interface view take effect on the interface only. Configurations made in Layer 2 aggregate interface view take effect only on the aggregate interface. Configurations made on an aggregation member port can take effect only after the port is removed from the aggregation group.
- After you enable a spanning tree protocol on a Layer 2 aggregate interface, the system performs spanning tree calculation on the Layer 2 aggregate interface. It does not perform spanning tree calculation on the aggregation member ports. The spanning tree protocol enable state and forwarding state of each selected member port is consistent with those of the corresponding Layer 2 aggregate interface.
- The member ports of an aggregation group do not participate in spanning tree calculation. However, the ports still reserve their spanning tree configurations for participating in spanning tree calculation after leaving the aggregation group.

STP configuration task list

Tasks at a glance
Configuring the root bridge: • (Required.) Setting the spanning tree mode • (Optional.) Configuring the root bridge or a secondary root bridge • (Optional.) Configuring the device priority • (Optional.) Configuring the network diameter of a switched network • (Optional.) Configuring spanning tree timers • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
Configuring the leaf nodes: • (Required.) Setting the spanning tree mode • (Optional.) Configuring the device priority • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring path costs of ports • (Optional.) Configuring the port priority • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
(Optional.) Configuring TC Snooping
(Optional.) Configuring protection functions

RSTP configuration task list

Tasks at a glance
Configuring the root bridge: • (Required.) Setting the spanning tree mode • (Optional.) Configuring the root bridge or a secondary root bridge • (Optional.) Configuring the device priority • (Optional.) Configuring the network diameter of a switched network • (Optional.) Configuring spanning tree timers • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring edge ports • (Optional.) Configuring the port link type • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
Configuring the leaf nodes: • (Required.) Setting the spanning tree mode • (Optional.) Configuring the device priority • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring edge ports • (Optional.) Configuring path costs of ports

Tasks at a glance
• (Optional.) Configuring the port priority • (Optional.) Configuring the port link type • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
(Optional.) Performing mCheck
(Optional.) Configuring TC Snooping
(Optional.) Configuring protection functions

PVST configuration task list

Tasks at a glance
Configuring the root bridge: • (Required.) Setting the spanning tree mode • (Optional.) Configuring the root bridge or a secondary root bridge • (Optional.) Configuring the device priority • (Optional.) Configuring the network diameter of a switched network • (Optional.) Configuring spanning tree timers • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring edge ports • (Optional.) Configuring the port link type • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
Configuring the leaf nodes: • (Required.) Setting the spanning tree mode • (Optional.) Configuring the device priority • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring edge ports • (Optional.) Configuring path costs of ports • (Optional.) Configuring the port priority • (Optional.) Configuring the port link type • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
(Optional.) Performing mCheck
(Optional.) Configuring protection functions

MSTP configuration task list

Tasks at a glance
Configuring the root bridge: • (Required.) Setting the spanning tree mode • (Required.) Configuring an MST region • (Optional.) Configuring the root bridge or a secondary root bridge • (Optional.) Configuring the device priority

Tasks at a glance
• (Optional.) Configuring the maximum hops of an MST region • (Optional.) Configuring the network diameter of a switched network • (Optional.) Configuring spanning tree timers • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring edge ports • (Optional.) Configuring the port link type • (Optional.) Configuring the mode a port uses to recognize and send MSTP packets • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
Configuring the leaf nodes: • (Required.) Setting the spanning tree mode • (Required.) Configuring an MST region • (Optional.) Configuring the device priority • (Optional.) Configuring the timeout factor • (Optional.) Configuring the BPDU transmission rate • (Optional.) Configuring edge ports • (Optional.) Configuring path costs of ports • (Optional.) Configuring the port priority • (Optional.) Configuring the port link type • (Optional.) Configuring the mode a port uses to recognize and send MSTP packets • (Optional.) Enabling outputting port state transition information • (Required.) Enabling the spanning tree feature
(Optional.) Performing mCheck
(Optional.) Configuring Digest Snooping
(Optional.) Configuring No Agreement Check
(Optional.) Configuring TC Snooping
(Optional.) Configuring protection functions

Setting the spanning tree mode

The spanning tree modes include:

- **STP mode**—All ports of the device send STP BPDUs. Select this mode when the peer device of a port supports only STP.
- **RSTP mode**—All ports of the device send RSTP BPDUs. A port in this mode automatically transits to the STP mode when it receives STP BPDUs from the peer device. A port in this mode does not transit to the MSTP mode when it receives MSTP BPDUs from the peer device.
- **MSTP mode**—All ports of the device send MSTP BPDUs. A port in this mode automatically transits to the STP mode when receiving STP BPDUs from the peer device. A port in this mode does not transit to the RSTP mode when receiving RSTP BPDUs from the peer device.
- **PVST mode**—All ports of the device send PVST BPDUs. Each VLAN maintains a spanning tree. In a network, the amount of spanning trees maintained by all devices equals the number of PVST-enabled VLANs multiplied by the number of PVST-enabled ports. If the amount of spanning trees exceeds the capacity of the network, device CPUs will be overloaded. Packet forwarding is interrupted, and the network becomes unstable. The device supports 128 PVST-enabled VLANs.

The MSTP mode is compatible with the RSTP mode, and the RSTP mode is compatible with the STP mode.

Compatibility of the PVST mode depends on the link type of a port.

- On an access port, the PVST mode is compatible with other spanning tree modes in all VLANs.
- On a trunk port or hybrid port, the PVST mode is compatible with other spanning tree modes only in VLAN 1.

To set the spanning tree mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the spanning tree mode.	**stp mode** { **mstp** |**pvst** | **rstp** | **stp** }	The default setting is the MSTP mode.

Configuring an MST region

Spanning tree devices belong to the same MST region if they are both connected through a physical link and configured with the following details:

- Format selector (0 by default, not configurable).
- MST region name.
- MST region revision level.
- VLAN-to-instance mapping entries in the MST region.

The configuration of MST region-related parameters (especially the VLAN-to-instance mapping table) might cause MSTP to begin a new spanning tree calculation. To reduce the possibility of topology instability, the MST region configuration takes effect only after you activate it by doing one of the following:

- Use the **active region-configuration** command.
- Enable a spanning tree protocol by using the **stp global enable** command if the spanning tree protocol is disabled.

In STP, RSTP, or PVST mode, MST region configurations do not take effect.

To configure an MST region:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MST region view.	**stp region-configuration**	N/A
3. Configure the MST region name.	**region-name** *name*	The default setting is the MAC address.
4. Configure the VLAN-to-instance mapping table.	• **instance** *instance-id* **vlan** *vlan-id-list* • **vlan-mapping modulo** *modulo*	Use one of the commands. By default, all VLANs in an MST region are mapped to the CIST (or MSTI 0).
5. Configure the MSTP revision level of the MST region.	**revision-level** *level*	The default setting is 0.
6. (Optional.) Display the MST region configurations that are not activated yet.	**check region-configuration**	N/A
7. Manually activate MST	**active region-configuration**	N/A

Step	Command	Remarks
region configuration.		

Configuring the root bridge or a secondary root bridge

You can have the spanning tree protocol determine the root bridge of a spanning tree through calculation. You can also specify the current device as the root bridge or as a secondary root bridge.

A device has independent roles in different spanning trees. It can act as the root bridge in one spanning tree and as a secondary root bridge in another. However, one device cannot be the root bridge and a secondary root bridge in the same spanning tree.

A spanning tree can have only one root bridge. If multiple devices can be selected as the root bridge in a spanning tree, the device with the lowest MAC address is chosen.

When the root bridge of an instance fails or is shut down and no new root bridge is specified, the following events occur:

- If you specify only one secondary root bridge for the instance, it becomes the root bridge.
- If you specify multiple secondary root bridges for the instance, the secondary root bridge with the lowest MAC address is given priority.
- If you do not specify a secondary root bridge, a new root bridge is calculated.

You can specify one root bridge for each spanning tree, regardless of the device priority settings. Once you specify a device as the root bridge or a secondary root bridge, you cannot change its priority.

You can configure the current device as the root bridge by setting the device priority to 0. For the device priority configuration, see "Configuring the device priority."

Configuring the current device as the root bridge of a specific spanning tree

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the current device as the root bridge.	• In STP/RSTP mode: **stp root primary** • In PVST mode: **stp vlan** *vlan-id-list* **root primary** • In MSTP mode: **stp** [**instance** *instance-list*] **root primary**	By default, a device does not function as the root bridge.

Configuring the current device as a secondary root bridge of a specific spanning tree

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Configure the current device as a secondary root bridge.	• In STP/RSTP mode: **stp root secondary** • In PVST mode: **stp vlan** *vlan-id-list* **root secondary** • In MSTP mode: **stp** [**instance** *instance-list*] **root secondary**	By default, a device does not function as a secondary root bridge.

Configuring the device priority

Device priority is a factor in calculating the spanning tree. The priority of a device determines whether the device can be elected as the root bridge of a spanning tree. A lower value indicates a higher priority. You can set the priority of a device to a low value to specify the device as the root bridge of the spanning tree. A spanning tree device can have different priorities in different spanning trees.

During root bridge selection, if all devices in a spanning tree have the same priority, the one with the lowest MAC address is selected. You cannot change the priority of a device after it is configured as the root bridge or as a secondary root bridge.

To configure the priority of a device in a specified MSTI:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the priority of the current device.	• In STP/RSTP mode: **stp priority** *priority* • In PVST mode: **stp vlan** *vlan-id-list* **priority** *priority* • In MSTP mode: **stp** [**instance** *instance-list*] **priority** *priority*	The default setting is 32768.

Configuring the maximum hops of an MST region

Restrict the region size by setting the maximum hops of an MST region. The hop limit configured on the regional root bridge is used as the hop limit for the MST region.

Configuration BPDUs sent by the regional root bridge always have a hop count set to the maximum value. When a device receives this configuration BPDU, it decrements the hop count by one, and uses the new hop count in the BPDUs that it propagates. When the hop count of a BPDU reaches zero, it is discarded by the device that received it. Devices beyond the reach of the maximum hops can no longer participate in spanning tree calculations, so the size of the MST region is limited.

Make this configuration only on the root bridge. All other devices in the MST region use the maximum hop value set for the root bridge.

You can configure the maximum hops of an MST region based on the STP network size. As a best practice, configure the maximum hops to a value that is greater than the maximum hops of each edge device to the root bridge.

To configure the maximum number of hops of an MST region:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the maximum hops of the MST region.	**stp max-hops** *hops*	The default setting is 20.

Configuring the network diameter of a switched network

Any two terminal devices in a switched network can reach each other through a specific path, and there are a series of devices on the path. The switched network diameter is the maximum number of devices on the path for an edge device to reach another one in the switched network through the root bridge. The network diameter indicates the network size. The bigger the diameter, the larger the network size.

Based on the network diameter you configured, the system automatically sets an optimal hello time, forward delay, and max age for the device.

In STP, RSTP, or MSTP mode, each MST region is considered a device. The configured network diameter takes effect only on the CIST (or the common root bridge) but not on other MSTIs.

In PVST mode, the configured network diameter takes effect only on the root bridges of the specified VLANs.

To configure the network diameter of a switched network:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the network diameter of the switched network.	• In STP/RSTP/MSTP mode: **stp bridge-diameter** *diameter* • In PVST mode: **stp vlan** *vlan-id-list* **bridge-diameter** *diameter*	The default setting is 7.

Configuring spanning tree timers

The following timers are used for spanning tree calculation:

- **Forward delay**—Delay time for port state transition. To prevent temporary loops on a network, the spanning tree feature sets an intermediate port state (the learning state) before it transits from the discarding state to the forwarding state. The feature also requires that the port transit its state after a forward delay timer to make sure the state transition of the local port stays synchronized with the peer.
- **Hello time**—Interval at which the device sends configuration BPDUs to detect link failures. If the device receives no configuration BPDUs within the timeout period, it recalculates the spanning tree. The formula for calculating the timeout period is timeout period = timeout factor × 3 × hello time.
- **Max age**—In the CIST of an MSTP network, the device uses the max age timer to determine if a configuration BPDU received by a port has expired. If it has, a new spanning tree calculation process starts. The max age timer does not take effect on other MSTIs except the CIST.

To ensure a fast topology convergence, make sure the timer settings meet the following formulas:

- 2 × (forward delay – 1 second) ≥ max age

- Max age ≥ 2 × (hello time + 1 second)

As a best practice, do not manually set the spanning tree timers. Instead, specify the network diameter and let spanning tree protocols automatically calculate the timers based on the network diameter. If the network diameter uses the default value, the timers also use their default values.

Configure the timers only on the root bridge. The timer settings on the root bridge apply to all devices on the entire switched network.

Configuration restrictions and guidelines

- The length of the forward delay timer is related to the network diameter of the switched network. The larger the network diameter is, the longer the forward delay time should be. If the forward delay timer is too short, temporary redundant paths might occur. If the forward delay timer is too long, network convergence might take a long time. As a best practice, use the automatically calculated value.
- An appropriate hello time setting enables the device to promptly detect link failures on the network without using excessive network resources. If the hello time is too long, the device mistakes packet loss for a link failure and triggers a new spanning tree calculation process. If the hello time is too short, the device frequently sends the same configuration BPDUs, which wastes device and network resources. As a best practice, use the automatically calculated value.
- If the max age timer is too short, the device frequently begins spanning tree calculations and might mistake network congestion as a link failure. If the max age timer is too long, the device might fail to promptly detect link failures and quickly launch spanning tree calculations, reducing the auto-sensing capability of the network. As a best practice, use the automatically calculated value.

Configuration procedure

To configure the spanning tree timers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the forward delay timer.	• In STP/RSTP/MSTP mode: **stp timer forward-delay** *time* • In PVST mode: **stp vlan** *vlan-id-list* **timer forward-delay** *time*	The default setting is 15 seconds.
3. Configure the hello timer.	• In STP/RSTP/MSTP mode: **stp timer hello** *time* • In PVST mode: **stp vlan** *vlan-id-list* **timer hello** *time*	The default setting is 2 seconds.
4. Configure the max age timer.	• In STP/RSTP/MSTP mode: **stp timer max-age** *time* • In PVST mode: **stp vlan** *vlan-id-list* **timer max-age** *time*	The default setting is 20 seconds.

Configuring the timeout factor

The timeout factor is a parameter used to decide the timeout period. The formula for calculating the timeout period is: timeout period = timeout factor × 3 × hello time.

In a stable network, each non-root-bridge device forwards configuration BPDUs to the downstream devices at the hello time interval to detect link failures. If a device does not receive a BPDU from the upstream device within nine times the hello time, it assumes that the upstream device has failed. Then, it starts a new spanning tree calculation process.

A device might fail to receive a BPDU from the upstream device because the upstream device is busy. If a spanning tree calculation occurs, the calculation can fail and also waste network resources. On a stable network, you can prevent undesired spanning tree calculations by setting the timeout factor to 5, 6, or 7.

To configure the timeout factor:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the timeout factor of the device.	**stp timer-factor** *factor*	The default setting is 3.

Configuring the BPDU transmission rate

The maximum number of BPDUs a port can send within each hello time equals the BPDU transmission rate plus the hello timer value. Configure an appropriate BPDU transmission rate based on the physical status of the port and the network structure.

The higher the BPDU transmission rate, the more BPDUs are sent within each hello time, and the more system resources are used. By setting an appropriate BPDU transmission rate, you can limit the rate at which the port sends BPDUs. Setting an appropriate rate also prevents spanning tree protocols from using excessive network resources when the network topology changes. As a best practice, use the default setting.

To configure the BPDU transmission rate:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the BPDU transmission rate of the ports.	**stp transmit-limit** *limit*	The default setting is 10.

Configuring edge ports

If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When network topology change occurs, an edge port will not cause a temporary loop. Because a device does not determine whether a port is directly connected to a terminal, you must manually configure the port as an edge port. After that, the port can rapidly transit from the blocked state to the forwarding state.

Configuration restrictions and guidelines

- If BPDU guard is disabled, a port set as an edge port becomes a non-edge port again if it receives a BPDU from another port. To restore the edge port, re-enable it.
- If a port directly connects to a user terminal, configure it as an edge port and enable BPDU guard for it. This enables the port to quickly transit to the forwarding state when ensuring network security.
- On a port, the loop guard function and the edge port setting are mutually exclusive.

Configuration procedure

To configure a port as an edge port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the current ports as edge ports.	**stp edged-port**	By default, all ports are non-edge ports.

Configuring path costs of ports

Path cost is a parameter related to the rate of a port. On a spanning tree device, a port can have different path costs in different MSTIs. Setting appropriate path costs allows VLAN traffic flows to be forwarded along different physical links, achieving VLAN-based load balancing.

You can have the device automatically calculate the default path cost, or you can configure the path cost for ports.

Specifying a standard for the device to use when it calculates the default path cost

CAUTION:

If you change the standard that the device uses to calculate the default path costs, you restore the path costs to the default.

You can specify a standard for the device to use in automatic calculation for the default path cost. The device supports the following standards:

- **dot1d-1998**—The device calculates the default path cost for ports based on IEEE 802.1d-1998.
- **dot1t**—The device calculates the default path cost for ports based on IEEE 802.1t.
- **legacy**—The device calculates the default path cost for ports based on a private standard.

When you specify a standard for the device to use when it calculates the default path cost, follow these guidelines:

- When it calculates the path cost for an aggregate interface, IEEE 802.1t takes into account the number of Selected ports in its aggregation group. However, IEEE 802.1d-1998 does not take into account the number of Selected ports. The calculation formula of IEEE 802.1t is: Path cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the Selected ports in the aggregation group.

- IEEE 802.1d-1998 or the private standard always assigns the smallest possible value to a single port or an aggregate interface when the link speed of the port or interface exceeds 10 Gbps. The forwarding path selected based on this criterion might not be the best one. To solve this problem, perform one of the following tasks:
  - Use **dot1t** as the standard for default path cost calculation.
  - Manually set the path cost for the port (see "Configuring path costs of ports").

To specify a standard for the device to use when it calculates the default path cost:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a standard for the device to use when it calculates the default path costs of its ports.	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	The default setting is **legacy**.

Table 9 Mappings between the link speed and the path cost

Link speed	Port type	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	Private standard
0	N/A	65535	200000000	200000
10 Mbps	Single port	100	2000000	2000
	Aggregate interface containing two Selected ports		1000000	1800
	Aggregate interface containing three Selected ports		666666	1600
	Aggregate interface containing four Selected ports		500000	1400
100 Mbps	Single port	19	200000	200
	Aggregate interface containing two Selected ports		100000	180
	Aggregate interface containing three Selected ports		66666	160
	Aggregate interface containing four Selected ports		50000	140
1000 Mbps	Single port	4	20000	20
	Aggregate interface containing two Selected ports		10000	18
	Aggregate interface containing three Selected ports		6666	16
	Aggregate interface containing four Selected		5000	14

Link speed	Port type	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	Private standard
	ports			
10 Gbps	Single port	2	2000	2
	Aggregate interface containing two Selected ports		1000	1
	Aggregate interface containing three Selected ports		666	1
	Aggregate interface containing four Selected ports		500	1
20 Gbps	Single port	1	1000	1
	Aggregate interface containing two Selected ports		500	1
	Aggregate interface containing three Selected ports		333	1
	Aggregate interface containing four Selected ports		250	1
40 Gbps	Single port	1	500	1
	Aggregate interface containing two Selected ports		250	1
	Aggregate interface containing three Selected ports		166	1
	Aggregate interface containing four Selected ports		125	1
100 Gbps	Single port	1	200	1
	Aggregate interface containing two Selected ports		100	1
	Aggregate interface containing three Selected ports		66	1
	Aggregate interface containing four Selected ports		50	1

Configuring path costs of ports

When the path cost of a port changes, the system recalculates the role of the port and initiates a state transition.

To configure the path cost of a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the path cost of the ports.	• In STP/RSTP mode: **stp cost** *cost* • In PVST mode: **stp vlan** *vlan-id-list* **cost** *cost* • In MSTP mode: **stp** [**instance** *instance-list*] **cost** *cost*	By default, the system automatically calculates the path cost of each port.

Configuration example

In MSTP mode, perform the following tasks:

- Configure the device to calculate the default path costs of its ports by using IEEE 802.1d-1998.
- Set the path cost of GigabitEthernet 1/0/3 to 200 on MSTI 2.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change the
current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated.
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 cost 200
```

In PVST mode, perform the following tasks:

- Configure the device to calculate the default path costs of its ports by using IEEE 802.1d-1998.
- Set the path cost of GigabitEthernet 1/0/3 to 2000 on VLAN 20 through VLAN 30.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change the
current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp vlan 20 to 30 cost 2000
```

Configuring the port priority

The priority of a port is a factor that determines whether the port can be elected as the root port of a device. If all other conditions are the same, the port with the highest priority is elected as the root port.

On a spanning tree device, a port can have different priorities and play different roles in different spanning trees. As a result, data of different VLANs can be propagated along different physical paths, implementing per-VLAN load balancing. You can set port priority values based on the actual networking requirements.

When the priority of a port changes, the system recalculates the port role and initiates a state transition.

To configure the priority of a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the port priority.	• In STP/RSTP mode: **stp port priority** *priority* • In PVST mode: **stp vlan** *vlan-id-list* **port priority** *priority* • In MSTP mode: **stp** [**instance** *instance-list*] **port priority** *priority*	The default setting is 128 for all ports.

Configuring the port link type

A point-to-point link directly connects two devices. If two root ports or designated ports are connected over a point-to-point link, they can rapidly transit to the forwarding state after a proposal-agreement handshake process.

Configuration restrictions and guidelines

- You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that operates in full duplex mode. As a best practice, use the default setting and let the device automatically detect the port link type.
- The **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port in MSTP or PVST mode takes effect on all MSTIs or VLANs.
- If you configure a non-point-to-point link as a point-to-point link, a temporary loop might occur.

Configuration procedure

To configure the link type of a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the port link type.	**stp point-to-point** { **auto** | **force-false** | **force-true** }	By default, the link type is **auto** where the port automatically detects the link type.

Configuring the mode a port uses to recognize and send MSTP packets

A port can receive and send MSTP packets in the following formats:

- **dot1s**—802.1s-compliant standard format

- **legacy**—Compatible format

By default, the packet format recognition mode of a port is **auto**. The port automatically distinguishes the two MSTP packet formats, and determines the format of packets that it will send based on the recognized format.

You can configure the MSTP packet format on a port. Then, the port sends only MSTP packets of the configured format to communicate with devices that send packets of the same format.

By default, a port in **auto** mode sends 802.1s MSTP packets. When the port receives an MSTP packet of a legacy format, the port starts to send packets only of the legacy format. This prevents the port from frequently changing the format of sent packets. To configure the port to send 802.1s MSTP packets, shut down and then bring up the port.

When the number of existing MSTIs exceeds 48, the port can send only 802.1s MSTP packets.

To configure the MSTP packet format to be supported on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the mode that the port uses to recognize/send MSTP packets.	**stp compliance** { **auto** | **dot1s** | **legacy** }	The default setting is **auto**.

Enabling outputting port state transition information

In a large-scale spanning tree network, you can enable devices to output the port state transition information. Then you can monitor the port states in real time.

To enable outputting port state transition information:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable outputting port state transition information.	• In STP/RSTP mode: **stp port-log instance 0** • In PVST mode: **stp port-log vlan** *vlan-id-list* • In MSTP mode: **stp port-log** { **all** | **instance** *instance-list* }	By default, this function is disabled.

Enabling the spanning tree feature

You must enable the spanning tree feature for the device before any other spanning tree related configurations can take effect. In STP, RSTP, or MSTP mode, make sure the spanning tree feature is enabled globally and on the desired ports. In PVST mode, make sure the spanning tree feature is enabled globally, in the desired VLANs, and on the desired ports.

You can disable the spanning tree feature for certain ports with the **undo stp enable** command to exclude them from spanning tree calculation and save CPU resources of the device. Make sure no loops occur in the network after you disable the spanning tree feature on these ports.

Enabling the spanning tree feature in STP/RSTP/MSTP mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the spanning tree feature.	**stp global enable**	• If the device starts up with the initial settings, the spanning tree feature is disabled globally by default. • If the device starts up with the factory defaults, the spanning tree feature is enabled globally by default. For more information about the startup configuration, see *Fundamentals Configuration Guide*.
3. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
4. (Optional.) Enable the spanning tree feature for the port.	**stp enable**	By default, the spanning tree feature is enabled on all ports.

Enabling the spanning tree feature in PVST mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the spanning tree feature.	**stp global enable**	• If the device starts up with the initial settings, the spanning tree feature is disabled globally by default. • If the device starts up with the factory defaults, the spanning tree feature is enabled globally by default. For more information about the startup configuration, see *Fundamentals Configuration Guide*.
3. Enable the spanning tree feature in VLANs.	**stp vlan** *vlan-id-list* **enable**	The spanning tree feature is enabled for all VLANs.
4. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
5. Enable the spanning tree feature on the port.	**stp enable**	By default, the spanning tree feature is enabled on all ports.

Performing mCheck

The mCheck feature enables user intervention in the port status transition process.

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.

- The port cannot detect the change.

To forcibly transit the port to operate in the original mode, you can perform an mCheck operation.

For example, Device A, Device B, and Device C are connected in sequence. Device A runs STP, Device B does not run any spanning tree protocol, and Device C runs RSTP, PVST, or MSTP. In this case, when Device C receives an STP BPDU transparently transmitted by Device B, the receiving port transits to the STP mode. If you configure Device B to run RSTP, PVST, or MSTP with Device C, you must perform mCheck operations on the ports interconnecting Device B and Device C.

Configuration restrictions and guidelines

When you configure mCheck, follow these restrictions and guidelines: The mCheck operation takes effect on devices operating in MSTP, PVST, or RSTP mode.

Configuration procedure

Performing mCheck globally

Step	Command
1. Enter system view.	**system-view**
2. Perform mCheck.	**stp global mcheck**

Performing mCheck in interface view

Step	Command
1. Enter system view.	**system-view**
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*
3. Perform mCheck.	**stp mcheck**

Configuring Digest Snooping

CAUTION:

Use caution with global Digest Snooping in the following situations:

- When you modify the VLAN-to-instance mappings.
- When you restore the default MST region configuration.

If the local device has different VLAN-to-instance mappings than its neighboring devices, loops or traffic interruption will occurs.

As defined in IEEE 802.1s, connected devices are in the same region only when they have the same MST region-related configurations, including:

- Region name.
- Revision level.
- VLAN-to-instance mappings.

A spanning tree device identifies devices in the same MST region by determining the configuration ID in BPDU packets. The configuration ID includes the region name, revision level, and configuration

digest. It is 16-byte long and is the result calculated through the HMAC-MD5 algorithm based on VLAN-to-instance mappings.

Because spanning tree implementations vary by vendor, the configuration digests calculated through private keys are different. The devices of different vendors in the same MST region cannot communicate with each other.

To enable communication between an HPE device and a third-party device in the same MST region, enable Digest Snooping on the HPE device port connecting them.

Configuration restrictions and guidelines

When you configure Digest Snooping, follow these restrictions and guidelines:

- Before you enable Digest Snooping, make sure associated devices of different vendors are connected and run spanning tree protocols.
- With Digest Snooping enabled, in-the-same-region verification does not require comparison of configuration digest. The VLAN-to-instance mappings must be the same on associated ports.
- To make Digest Snooping take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, enable Digest Snooping on all associated ports first and then enable it globally. This will make the configuration take effect on all configured ports and reduce impact on the network.
- To prevent loops, do not enable Digest Snooping on MST region edge ports.
- As a best practice, enable Digest Snooping first and then the spanning tree feature. To avoid traffic interruption, do not configure Digest Snooping when the network is already working well.

Configuration procedure

You can enable Digest Snooping only on the HPE device that is connected to a third-party device that uses its private key to calculate the configuration digest.

To configure Digest Snooping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable Digest Snooping on the interface.	**stp config-digest-snooping**	By default, Digest Snooping is disabled on ports.
4. Return to system view.	**quit**	N/A
5. Enable Digest Snooping globally.	**stp global config-digest-snooping**	By default, Digest Snooping is disabled globally.

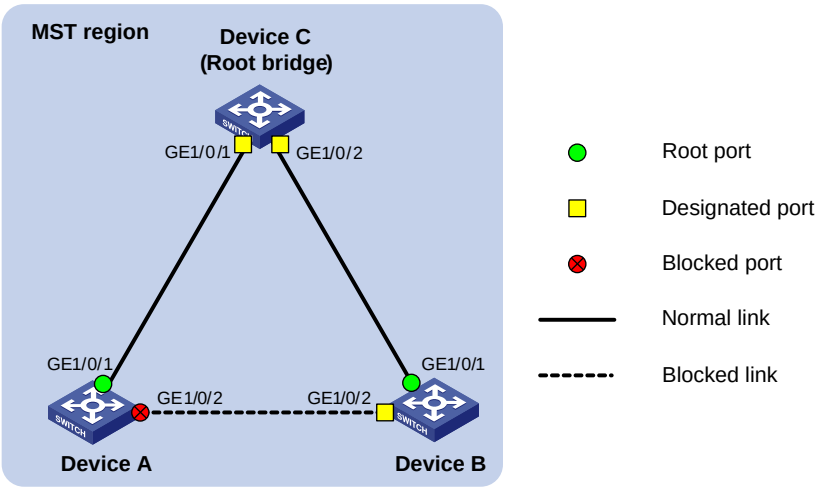
Digest Snooping configuration example

Network requirements

As shown in Figure 26, Device A and Device B connect to Device C, which is a third-party device. All these devices are in the same region.

Enable Digest Snooping on the ports of Device A and Device B that connect to Device C, so that the three devices can communicate with one another.

Figure 26 Network diagram



Configuration procedure

Enable Digest Snooping on GigabitEthernet 1/0/1 of Device A and enable global Digest Snooping on Device A.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] stp global config-digest-snooping
```

Enable Digest Snooping on GigabitEthernet 1/0/1 of Device B and enable global Digest Snooping on Device B.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] stp global config-digest-snooping
```

Configuring No Agreement Check

In RSTP and MSTP, the following types of messages are used for rapid state transition on designated ports:

- **Proposal**—Sent by designated ports to request rapid transition
- **Agreement**—Used to acknowledge rapid transition requests

Both RSTP and MSTP devices can perform rapid transition on a designated port only when the port receives an agreement packet from the downstream device. RSTP and MSTP devices have the following differences:

- For MSTP, the root port of the downstream device sends an agreement packet only after it receives an agreement packet from the upstream device.
- For RSTP, the downstream device sends an agreement packet regardless of whether an agreement packet from the upstream device is received.

Figure 27 Rapid state transition of an MSTP designated port

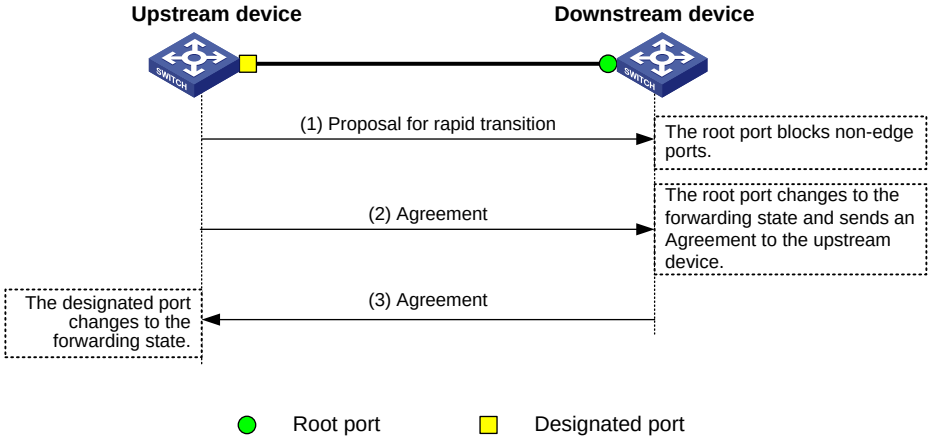
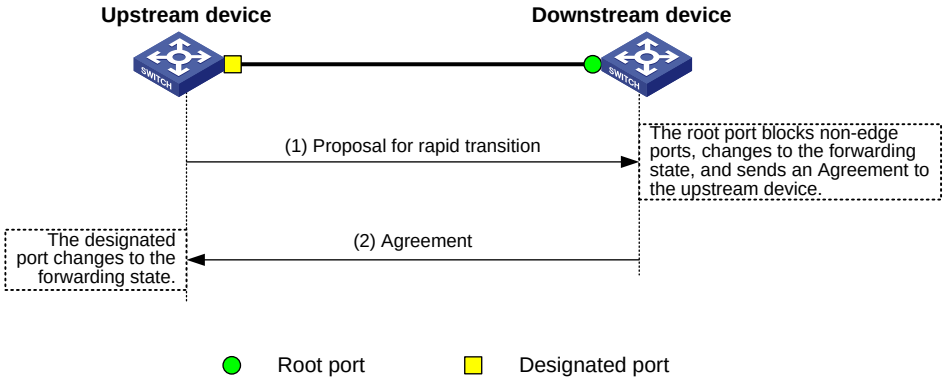


Figure 28 Rapid state transition of an RSTP designated port



If the upstream device is a third-party device, the rapid state transition implementation might be limited as follows:

- The upstream device uses a rapid transition mechanism similar to that of RSTP.
- The downstream device adopts MSTP and does not operate in RSTP mode.

In this case, the following occurs:

1. The root port on the downstream device receives no agreement packet from the upstream device.
2. It sends no agreement packets to the upstream device.

As a result, the designated port of the upstream device can transit to the forwarding state only after a period twice the Forward Delay.

You can enable the No Agreement Check feature on the downstream device's port to enable the designated port of the upstream device to transit its state rapidly.

Configuration prerequisites

Before you configure the No Agreement Check function, complete the following tasks:

- Connect a device to a third-party upstream device that supports spanning tree protocols through a point-to-point link.
- Configure the same region name, revision level, and VLAN-to-instance mappings on the two devices.

Configuration procedure

Enable the No Agreement Check feature on the root port.

To configure No Agreement Check:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable No Agreement Check.	**stp no-agreement-check**	By default, No Agreement Check is disabled.

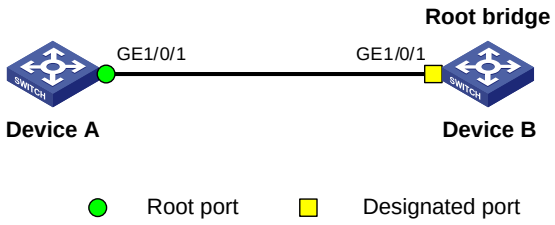
No Agreement Check configuration example

Network requirements

As shown in Figure 29, Device A connects to a third-party device that has a different spanning tree implementation. Both devices are in the same region.

The third-party device (Device B) is the regional root bridge, and Device A is the downstream device.

Figure 29 Network diagram



Configuration procedure

Enable No Agreement Check on GigabitEthernet 1/0/1 of Device A.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

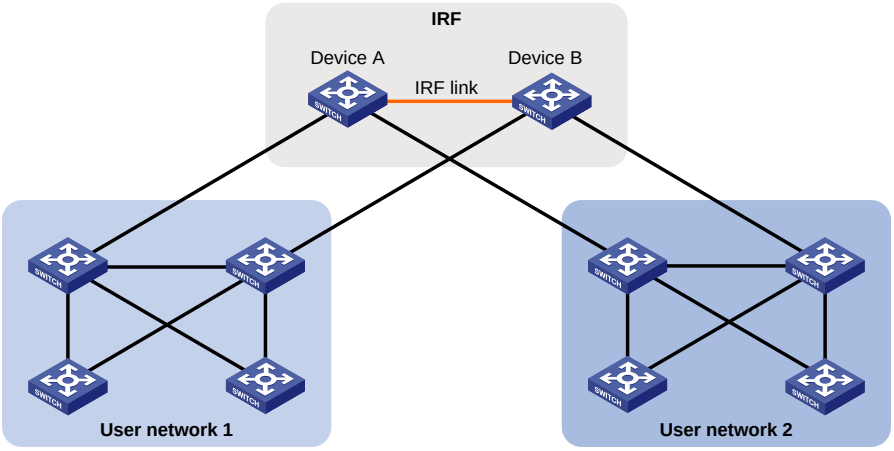
Configuring TC Snooping

As shown in Figure 30, an IRF fabric connects to two user networks through double links.

- Device A and Device B form an IRF fabric.
- The spanning tree feature is disabled on Device A and Device B and enabled on all devices in user network 1 and user network 2.
- The IRF fabric transparently transmits BPDUs for both user networks and is not involved in the calculation of spanning trees.

When the network topology changes, it takes time for the IRF fabric to update its MAC address table and ARP table. During this period, traffic in the network might be interrupted.

Figure 30 TC Snooping application scenario



To avoid traffic interruption, you can enable TC Snooping on the IRF fabric. After receiving a TC-BPDU through a port, the IRF fabric updates MAC address table and ARP table entries associated with the port's VLAN. In this way, TC Snooping prevents topology change from interrupting traffic forwarding in the network. For more information about the MAC address table and the ARP table, see "Configuring the MAC address table" and *Layer 3—IP Services Configuration Guide*.

Configuration restrictions and guidelines

When you configure TC Snooping, follow these restrictions and guidelines:

- TC Snooping and the spanning tree feature are mutually exclusive. You must globally disable the spanning tree feature before enabling TC Snooping.
- TC Snooping does not support the PVST mode.

Configuration procedure

To enable TC Snooping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Globally disable the spanning tree feature.	**undo stp global enable**	• If the device starts up with the initial settings, the spanning tree feature is disabled globally by default. • If the device starts up with the factory defaults, the spanning tree feature is enabled globally by default. For more information about the startup configuration, see *Fundamentals Configuration Guide*.
3. Enable TC Snooping.	**stp tc-snooping**	By default, TC Snooping is disabled.

Configuring protection functions

A spanning tree device supports the following protection functions:

- BPDU guard
- Root guard
- Loop guard
- Port role restriction
- TC-BPDU transmission restriction
- TC-BPDU guard
- BPDU drop

Enabling BPDU guard

For access layer devices, the access ports can directly connect to the user terminals (such as PCs) or file servers. The access ports are configured as edge ports to allow rapid transition. When these ports receive configuration BPDUs, the system automatically sets the ports as non-edge ports and starts a new spanning tree calculation process. This causes a change of network topology. Under normal conditions, these ports should not receive configuration BPDUs. However, if someone uses configuration BPDUs maliciously to attack the devices, the network will become unstable.

The spanning tree protocol provides the BPDU guard function to protect the system against such attacks. When edge ports receive configuration BPDUs on a device with BPDU guard enabled, the device performs the following tasks:

- Shuts down these ports.
- Notifies the NMS that these ports have been shut down by the spanning tree protocol.

The device reactivates the shutdown ports after a detection interval. For more information about this detection interval, see *Fundamentals Configuration Guide*.

BPDU guard does not take effect on loopback-testing-enabled ports. For more information about loopback testing, see "Configuring Ethernet interfaces."

Configure BPDU guard on a device with edge ports configured.

To enable BPDU guard:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the BPDU guard function for the device.	**stp bpdu-protection**	By default, BPDU guard is disabled.

Enabling root guard

The root bridge and secondary root bridge of a spanning tree should be located in the same MST region. Especially for the CIST, the root bridge and secondary root bridge are put in a high-bandwidth core region during network design. However, due to possible configuration errors or malicious attacks in the network, the legal root bridge might receive a configuration BPDU with a higher priority. Another device supersedes the current legal root bridge, causing an undesired change of the network topology. The traffic that should go over high-speed links is switched to low-speed links, resulting in network congestion.

To prevent this situation, MSTP provides the root guard function. If root guard is enabled on a port of a root bridge, this port plays the role of designated port on all MSTIs. After this port receives a configuration BPDU with a higher priority from an MSTI, it performs the following tasks:

- Immediately sets that port to the listening state in the MSTI.
- Does not forward the received configuration BPDU.

This is equivalent to disconnecting the link connected with this port in the MSTI. If the port receives no BPDUs with a higher priority within twice the forwarding delay, it reverts to its original state.

On a port, the loop guard function and the root guard function are mutually exclusive.

Configure root guard on a designated port.

To enable root guard:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the root guard function.	**stp root-protection**	By default, root guard is disabled.

Enabling loop guard

By continuing to receive BPDUs from the upstream device, a device can maintain the state of the root port and blocked ports. However, link congestion or unidirectional link failures might cause these ports to fail to receive BPDUs from the upstream devices. In this case, the device reselects the following port roles:

- Those ports in forwarding state that failed to receive upstream BPDUs become designated ports.
- The blocked ports transit to the forwarding state.

As a result, loops occur in the switched network. The loop guard function can suppress the occurrence of such loops.

The initial state of a loop guard-enabled port is **discarding** in every MSTI. When the port receives BPDUs, it transits its state. Otherwise, it stays in the discarding state to prevent temporary loops.

Do not enable loop guard on a port that connects user terminals. Otherwise, the port stays in the discarding state in all MSTIs because it cannot receive BPDUs.

On a port, the loop guard function is mutually exclusive with the root guard function or the edge port setting.

Configure loop guard on the root port and alternate ports of a device.

To enable loop guard:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the loop guard function for the ports.	**stp loop-protection**	By default, loop guard is disabled.

Configuring port role restriction

CAUTION:

Use this feature with caution, because enabling port role restriction on a port might affect the connectivity of the spanning tree topology.

The change to the bridge ID of a device in the user access network might cause a change to the spanning tree topology in the core network. To avoid this problem, you can enable port role restriction on a port. With this feature enabled, when the port receives a superior BPDU, it becomes an alternate port rather than a root port.

Make this configuration on the port that connects to the user access network.

To configure port role restriction:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable port role restriction.	**stp role-restriction**	By default, port role restriction is disabled.

Configuring TC-BPDU transmission restriction

CAUTION:

Enabling TC-BPDU transmission restriction on a port might cause the previous forwarding address table to fail to be updated when the topology changes.

The topology change to the user access network might cause the forwarding address changes to the core network. When the user access network topology is unstable, the user access network might affect the core network. To avoid this problem, you can enable TC-BPDU transmission restriction on a port. With this feature enabled, when the port receives a TC-BPDU, it does not forward the TC-BPDU to other ports.

Make this configuration on the port that connects to the user access network.

To configure TC-BPDU transmission restriction:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable TC-BPDU transmission restriction.	**stp tc-restriction**	By default, TC-BPDU transmission restriction is disabled.

Enabling TC-BPDU guard

When a device receives topology change (TC) BPDUs (the BPDUs that notify devices of topology changes), it flushes its forwarding address entries. If someone uses TC-BPDUs to attack the device, the device will receive a large number of TC-BPDUs within a short time and be busy with forwarding address entry flushing. This affects network stability.

TC-BPDU guard allows you to set the maximum number of immediate forwarding address entry flushes performed within 10 seconds after the device receives the first TC-BPDU. For TC-BPDUs received in excess of the limit, the device performs a forwarding address entry flush when the time period expires. This prevents frequent flushing of forwarding address entries. As a best practice, enable TC-BPDU guard.

To enable TC-BPDU guard:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the TC-BPDU guard function.	**stp tc-protection**	By default, TC-BPDU guard is enabled. As a best practice, do not disable this feature.
3. (Optional.) Configure the maximum number of forwarding address entry flushes that the device can perform every 10 seconds.	**stp tc-protection threshold** *number*	The default setting is 6.

Enabling BPDU drop

In a spanning tree network, every BPDU arriving at the device triggers an STP calculation process and is then forwarded to other devices in the network. Malicious attackers might use the vulnerability to attack the network by forging BPDUs. By continuously sending forged BPDUs, they can make all devices in the network continue performing STP calculations. As a result, problems such as CPU overload and BPDU protocol status errors occur.

To avoid this problem, you can enable BPDU drop on ports. A BPDU drop-enabled port does not receive any BPDUs and is invulnerable to forged BPDU attacks.

To enable BPDU drop on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable BPDU drop on the current interface.	**bpdu-drop any**	By default, BPDU drop is disabled.

About dispute guard

Dispute guard is enabled by default. You do not need to manually configure this feature.

Dispute guard can be triggered by unidirectional link failures. If an upstream port receives inferior BPDUs from a downstream designated port in forwarding or learning state because of a unidirectional link failure, a loop appears. Dispute guard blocks the upstream designated port to prevent the loop.

As shown in Figure 31, in normal conditions, the spanning tree calculation result is as follows:

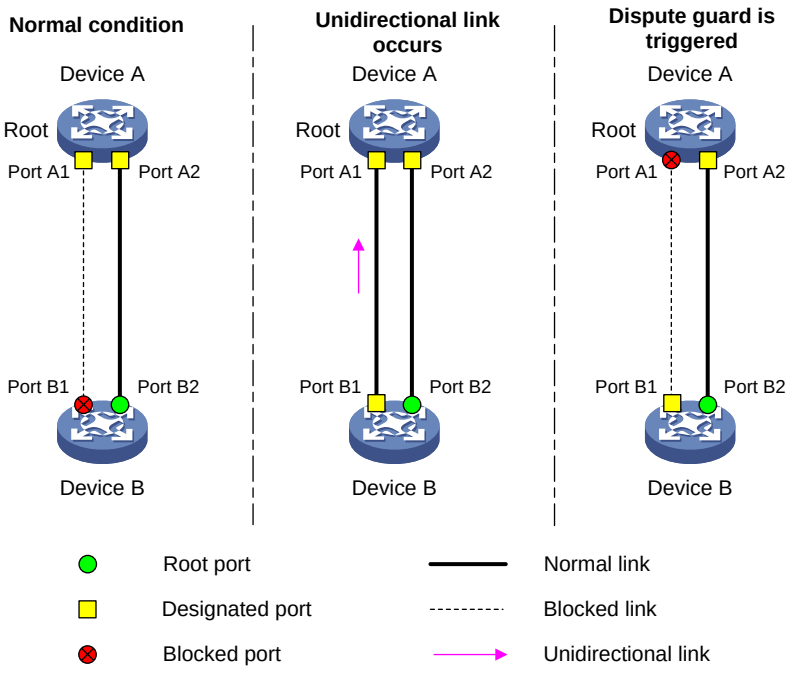
- Device A is the root bridge, and Port A1 is a designated port.
- Port B1 is blocked.

When the link between Port A1 and Port B1 fails in the direction of Port A1 to Port B1 and becomes unidirectional, the following events occur:

1. Port A1 can only receive BPDUs and cannot send BPDUs to Port B1.
2. Port B1 does not receive BPDUs from Port A1 for a certain period of time.
3. Device B determines itself as the root bridge.
4. Port B1 sends its BPDUs to Port A1.
5. Port A1 determines the received BPDUs are inferior to its own BPDUs. A dispute is detected.

6. Dispute guard is triggered and blocks Port A1 to prevent a loop.

Figure 31 Dispute guard triggering scenario



Displaying and maintaining the spanning tree

Execute **display** commands in any view and **reset** command in user view.

Task	Command
Display information about ports blocked by spanning tree protection functions.	**display stp abnormal-port**
Display BPDU statistics on ports.	**display stp bpdu-statistics** [**interface** *interface-type interface-number* [**instance** *instance-list*]]
Display information about ports shut down by spanning tree protection functions.	**display stp down-port**
Display the historical information of port role calculation for the specified MSTI or all MSTIs.	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]
Display the statistics of TC/TCN BPDUs sent and received by all ports in the specified MSTI or all MSTIs.	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]
Display the spanning tree status and statistics.	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]
Display the MST region configuration information that has taken effect.	**display stp region-configuration**
Display the root bridge information of all MSTIs.	**display stp root**
Clear the spanning tree statistics.	**reset stp** [**interface** *interface-list*]

Spanning tree configuration example

MSTP configuration example

Network requirements

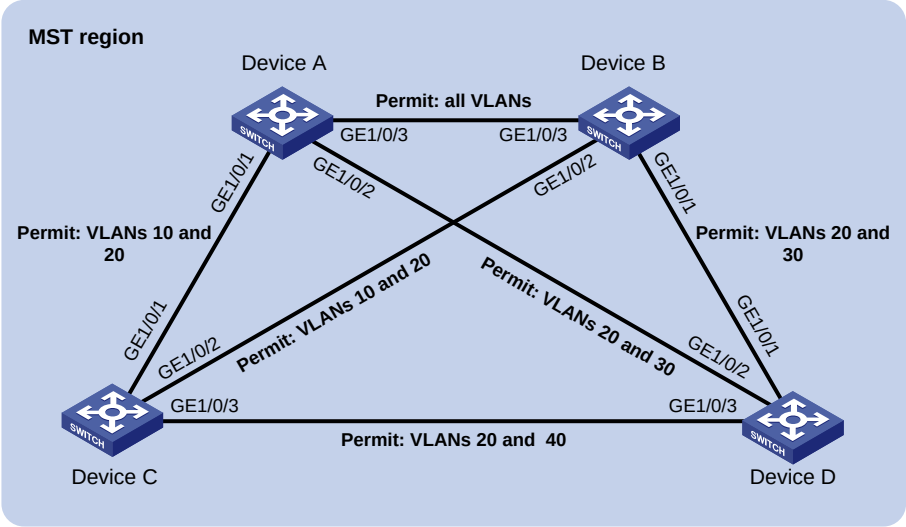
As shown in Figure 32, all devices on the network are in the same MST region. Device A and Device B work at the distribution layer. Device C and Device D work at the access layer.

Configure MSTP so that packets of different VLANs are forwarded along different spanning trees.

- VLAN 10 packets are forwarded along MSTI 1.
- VLAN 30 packets are forwarded along MSTI 3.
- VLAN 40 packets are forwarded along MSTI 4.
- VLAN 20 packets are forwarded along MSTI 0.

VLAN 10 and VLAN 30 are terminated on the distribution layer devices, and VLAN 40 is terminated on the access layer devices. The root bridges of MSTI 1 and MSTI 3 are Device A and Device B, respectively, and the root bridge of MSTI 4 is Device C.

Figure 32 Network diagram



Configuration procedure

1. Configure VLANs and VLAN member ports. (Details not shown.)
   - Create VLAN 10, VLAN 20, and VLAN 30 on both Device A and Device B.
   - Create VLAN 10, VLAN 20, and VLAN 40 on Device C.
   - Create VLAN 20, VLAN 30, and VLAN 40 on Device D.
   - Configure the ports on these devices as trunk ports and assign them to related VLANs.
2. Configure Device A:

   # Enter MST region view, and configure the MST region name as **example**.

   ```
   <DeviceA> system-view
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] region-name example
   ```

   # Map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4, respectively.

   ```
   [DeviceA-mst-region] instance 1 vlan 10
   ```

```
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
```

Configure the revision level of the MST region as 0.

```
[DeviceA-mst-region] revision-level 0
```

Activate MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Specify the device as the root bridge of MSTI 1.

```
[DeviceA] stp instance 1 root primary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

3. Configure Device B:

Enter MST region view, and configure the MST region name as **example**.

```
<DeviceB> system-view
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
```

Map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4, respectively.

```
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
```

Configure the revision level of the MST region as 0.

```
[DeviceB-mst-region] revision-level 0
```

Activate MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Specify the device as the root bridge of MSTI 3.

```
[DeviceB] stp instance 3 root primary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

4. Configure Device C:

Enter MST region view, and configure the MST region name as **example**.

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
```

Map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4, respectively.

```
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
```

Configure the revision level of the MST region as 0.

```
[DeviceC-mst-region] revision-level 0
```

Activate MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Specify the device as the root bridge of MSTI 4.

```
[DeviceC] stp instance 4 root primary
```

Enable the spanning tree feature globally.

```
[DeviceC] stp global enable
```

5. Configure Device D:

   # Enter MST region view, and configure the MST region name as **example**.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
```

   # Map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4, respectively.

```
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
```

   # Configure the revision level of the MST region as 0.

```
[DeviceD-mst-region] revision-level 0
```

   # Activate MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

   # Enable the spanning tree feature globally.

```
[DeviceD] stp global enable
```

Verifying the configuration

In this example, Device B has the lowest root bridge ID. As a result, Device B is elected as the root bridge in MSTI 0.

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
[DeviceA] display stp brief
 MST ID      Port                                    Role  STP State     Protection
 0           GigabitEthernet1/0/1                  ALTE  DISCARDING    NONE
 0           GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
 1           GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID      Port                                    Role  STP State     Protection
 0           GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
 3           GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
 MST ID      Port                                    Role  STP State     Protection
 0           GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/2                  ROOT  FORWARDING    NONE
```

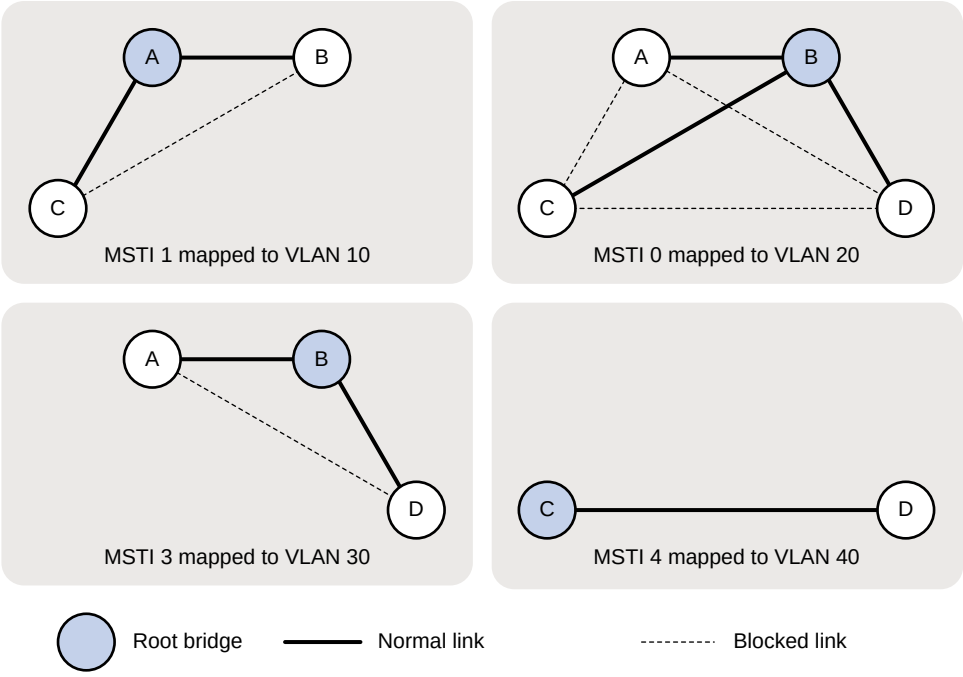
```
 0           GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/1                  ROOT  FORWARDING    NONE
 1           GigabitEthernet1/0/2                  ALTE  DISCARDING    NONE
 4           GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 MST ID      Port                                      Role  STP State     Protection
 0           GigabitEthernet1/0/1                  ROOT  FORWARDING    NONE
 0           GigabitEthernet1/0/2                  ALTE  DISCARDING    NONE
 0           GigabitEthernet1/0/3                  ALTE  DISCARDING    NONE
 3           GigabitEthernet1/0/1                  ROOT  FORWARDING    NONE
 3           GigabitEthernet1/0/2                  ALTE  DISCARDING    NONE
 4           GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
```

Based on the output, you can draw each MSTI mapped to each VLAN, as shown in Figure 33.

Figure 33 MSTIs mapped to different VLANs



PVST configuration example

Network requirements

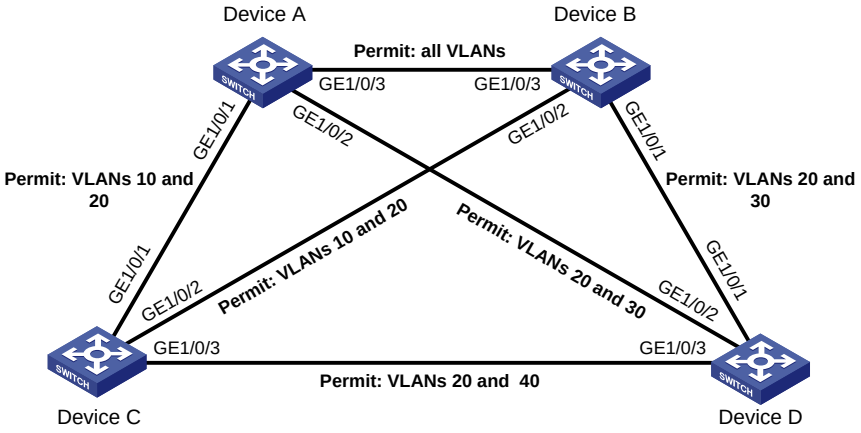
As shown in Figure 34, Device A and Device B work at the distribution layer, and Device C and Device D work at the access layer.

Configure PVST to meet the following requirements:

- Packets of a VLAN are forwarded along the spanning trees of the VLAN.
- VLAN 10, VLAN 20, and VLAN 30 are terminated on the distribution layer devices, and VLAN 40 is terminated on the access layer devices.
- The root bridge of VLAN 10 and VLAN 20 is Device A.
- The root bridge of VLAN 30 is Device B.

- The root bridge of VLAN 40 is Device C.

Figure 34 Network diagram



Configuration procedure

1. Configure VLANs and VLAN member ports. (Details not shown.)
   - Create VLAN 10, VLAN 20, and VLAN 30 on both Device A and Device B.
   - Create VLAN 10, VLAN 20, and VLAN 40 on Device C.
   - Create VLAN 20, VLAN 30, and VLAN 40 on Device D.
   - Configure the ports on these devices as trunk ports and assign them to related VLANs.
2. Configure Device A:

   # Set the spanning tree mode to PVST.

   ```
   <DeviceA> system-view
   [DeviceA] stp mode pvst
   ```

   # Configure the device as the root bridge of VLAN 10 and VLAN 20.

   ```
   [DeviceA] stp vlan 10 20 root primary
   ```

   # Enable the spanning tree feature globally and in VLAN 10, VLAN 20, and VLAN 30.

   ```
   [DeviceA] stp global enable
   [DeviceA] stp vlan 10 20 30 enable
   ```
3. Configure Device B:

   # Set the spanning tree mode to PVST.

   ```
   <DeviceB> system-view
   [DeviceB] stp mode pvst
   ```

   # Configure the device as the root bridge of VLAN 30.

   ```
   [DeviceB] stp vlan 30 root primary
   ```

   # Enable the spanning tree feature globally and in VLAN 10, VLAN 20, and VLAN 30.

   ```
   [DeviceB] stp global enable
   [DeviceB] stp vlan 10 20 30 enable
   ```
4. Configure Device C:

   # Set the spanning tree mode to PVST.

   ```
   <DeviceC> system-view
   [DeviceC] stp mode pvst
   ```

   # Configure the device as the root bridge of VLAN 40.

   ```
   [DeviceC] stp vlan 40 root primary
   ```

   # Enable the spanning tree feature globally and in VLAN 10, VLAN 20, and VLAN 40.

```
[DeviceC] stp global enable
[DeviceC] stp vlan 10 20 40 enable
```

5. Configure Device D:

   # Set the spanning tree mode to PVST.

```
<DeviceD> system-view
[DeviceD] stp mode pvst
```

   # Enable the spanning tree feature globally and in VLAN 20, VLAN 30, and VLAN 40.

```
[DeviceD] stp global enable
[DeviceD] stp vlan 20 30 40 enable
```

Verifying the configuration

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 VLAN ID     Port                                    Role  STP State     Protection
 10          GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 10          GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 VLAN ID     Port                                    Role  STP State     Protection
 10          GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 10          GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/2                  DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/3                  ROOT  FORWARDING    NONE
 30          GigabitEthernet1/0/1                  DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
 VLAN ID     Port                                    Role  STP State     Protection
 10          GigabitEthernet1/0/1                  ROOT  FORWARDING    NONE
 10          GigabitEthernet1/0/2                  ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/1                  ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/2                  ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
 40          GigabitEthernet1/0/3                  DESI  FORWARDING    NONE
```

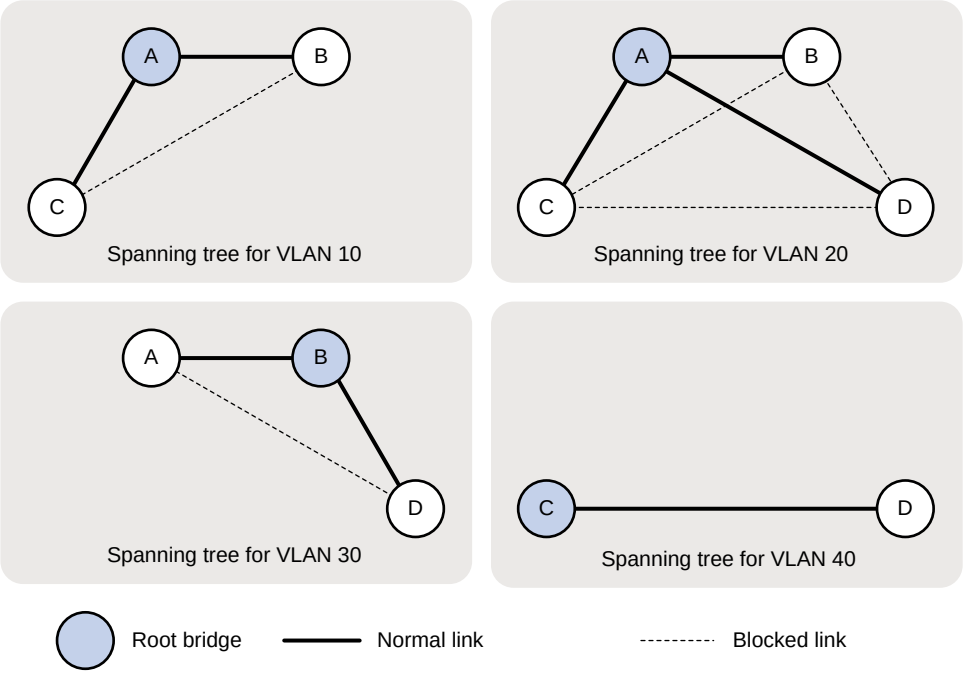
Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 VLAN ID     Port                                    Role  STP State     Protection
 20          GigabitEthernet1/0/1                  ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/2                  ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/3                  ALTE  DISCARDING    NONE
```

```
30          GigabitEthernet1/0/1                ROOT  FORWARDING    NONE
30          GigabitEthernet1/0/2                ALTE  DISCARDING    NONE
40          GigabitEthernet1/0/3                ROOT  FORWARDING    NONE
```

Based on the output, you can draw a topology for each VLAN spanning tree, as shown in Figure 35.

Figure 35 VLAN spanning tree topologies



Configuring loop detection

Overview

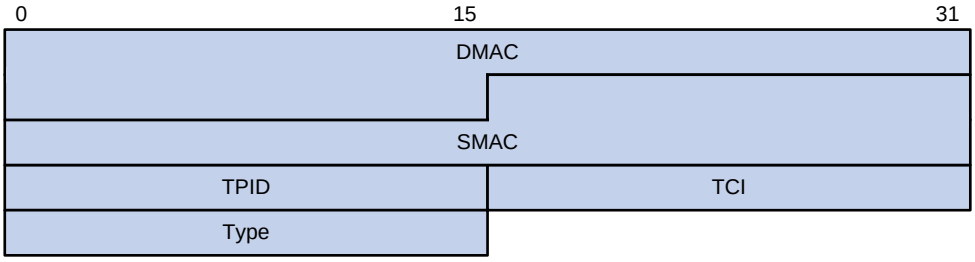
Incorrect network connections or configurations can create Layer 2 loops, which results in repeated transmission of broadcasts, multicasts, or unknown unicasts. The repeated transmission can waste network resources and can sometimes paralyze networks. The loop detection mechanism immediately generates a log when a loop occurs so that you are promptly notified to adjust network connections and configurations. You can configure loop detection to shut down the looped port. Logs are maintained in the information center. For more information, see *Network Management and Monitoring Configuration Guide*.

Loop detection mechanism

The device detects loops by sending detection frames and then checking whether these frames return to any port on the device. If they do, the device considers that the port is on a looped link.

Loop detection usually works within a VLAN. If a detection frame is returned with a VLAN tag different from the one it was sent out with, an inter-VLAN loop has occurred. To remove the loop, examine the QinQ configuration for incorrect settings. For more information about QinQ, see "Configuring QinQ.".

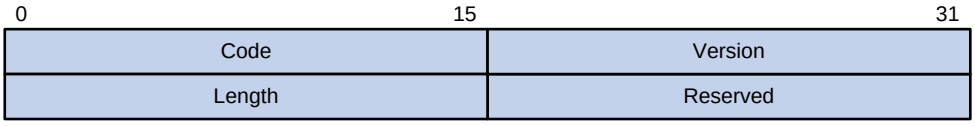
Figure 36 Ethernet frame header for loop detection



The Ethernet frame header for loop detection contains the following fields:

- **DMAC**—Destination MAC address of the frame, which is the multicast MAC address 010F-E200-0007. When a loop detection-enabled device receives a frame with this destination MAC address, it sends the frame to the CPU and floods the frame in the VLAN from which the frame was originally received.
- **SMAC**—Source MAC address of the frame, which is the bridge MAC address of the sending device.
- **TPID**—Type of the VLAN tag, with the value of 0x8100.
- **TCI**—Information of the VLAN tag, including the priority and VLAN ID.
- **Type**—Protocol type, with the value of 0x8918.

Figure 37 Inner frame header for loop detection



The inner frame header for loop detection contains the following fields:

- **Code**—Protocol sub-type, which is 0x0001, indicating the loop detection protocol.
- **Version**—Protocol version, which is always 0x0000.
- **Length**—Length of the frame. The value includes the inner header, but excludes the Ethernet header.
- **Reserved**—This field is reserved.

Frames for loop detection are encapsulated as TLV triplets.

Table 10 TLVs supported by loop detection

TLV	Description	Remarks
End of PDU	End of a PDU.	Optional.
Device ID	Bridge MAC address of the sending device.	Required.
Port ID	ID of the PDU sending port.	Optional.
Port Name	Name of the PDU sending port.	Optional.
System Name	Device name.	Optional.
Chassis ID	Chassis ID of the sending port.	Optional.
Slot ID	Slot ID of the sending port.	Optional.
Sub Slot ID	Sub-slot ID of the sending port.	Optional.

Loop detection interval

Loop detection is a continuous process as the network changes. Loop detection frames are sent at a specified interval (called a loop detection interval) to determine whether loops occur on ports and whether loops are removed.

Loop protection actions

When the switch detects a loop on a port, it generates a log but performs no action on the port by default. You can configure the switch to take one of the following actions:

- **Block**—Disables the port from learning MAC addresses and blocks inbound traffic to the port.
- **No-learning**—Disables the port from learning MAC addresses.
- **Shutdown**—Shuts down the port to disable it from receiving and sending any frames.

Port status auto recovery

When the device configured with the block or no-learning loop action detects a loop on a port, it performs the action and waits three loop detection intervals. If the device does not receive a loop detection frame within three loop detection intervals, it performs the following tasks:

- Automatically sets the port to the forwarding state.
- Notifies the user of the event.

When the device configured with the shutdown action detects a loop on a port, the following events occur:

1. The device automatically shuts down the port.

2. The device automatically sets the port to the forwarding state after the detection timer configured by using the **shutdown-interval** command expires. For more information about the **shutdown-interval** command, see *Fundamentals Command Reference*.
3. The device shuts down the port again if a loop is still detected on the port when the detection timer expires.

This process is repeated until the loop is removed.

NOTE:

Incorrect recovery can occur when loop detection frames are discarded to reduce the load. To avoid this problem, use the shutdown action or manually remove the loop.

Loop detection configuration task list

Tasks at a glance
(Required.) Enabling loop detection
(Optional.) Configuring the loop protection action
(Optional.) Setting the loop detection interval

Enabling loop detection

The loop protection action on a port can be triggered even if loop detection is disabled on the port when the following requirements are met:

- Loop detection is enabled globally or on any other port on the device.
- The port receives a loop detection frame of any VLAN.

Enabling loop detection globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Globally enable loop detection.	**loopback-detection global enable vlan** { *vlan-list* | **all** }	Disabled by default.

Enabling loop detection on a port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable loop detection on the port.	**loopback-detection enable vlan** { *vlan-list* | **all** }	Disabled by default.

Configuring the loop protection action

You can configure the loop protection action globally or on a per-port basis. The global configuration applies to all ports. The per-port configuration applies to the individual ports. The per-port configuration takes precedence over the global configuration.

Configuring the global loop protection action

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the global loop protection action.	**loopback-detection global action shutdown**	By default, the switch generates a log but performs no action on the port on which a loop is detected.

Configuring the loop protection action on a Layer 2 Ethernet interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the loop protection action on the interface.	**loopback-detection action** { **block** | **no-learning** | **shutdown** }	By default, the switch generates a log but performs no action on the port on which a loop is detected.

Configuring the loop protection action on a Layer 2 aggregate interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 aggregate interface view.	**interface bridge-aggregation** *interface-number*	N/A
3. Configure the loop protection action on the interface.	**loopback-detection action shutdown**	By default, the switch generates a log but performs no action on the port on which a loop is detected.

Setting the loop detection interval

With loop detection enabled, the switch sends loop detection frames at a specified interval. A shorter interval offers more sensitive detection but consumes more resources. Consider the system performance and loop detection speed when you set the loop detection interval.

To set the loop detection interval:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the loop detection interval.	**loopback-detection interval-time** *interval*	The default setting is 30 seconds.

Displaying and maintaining loop detection

Execute **display** commands in any view.

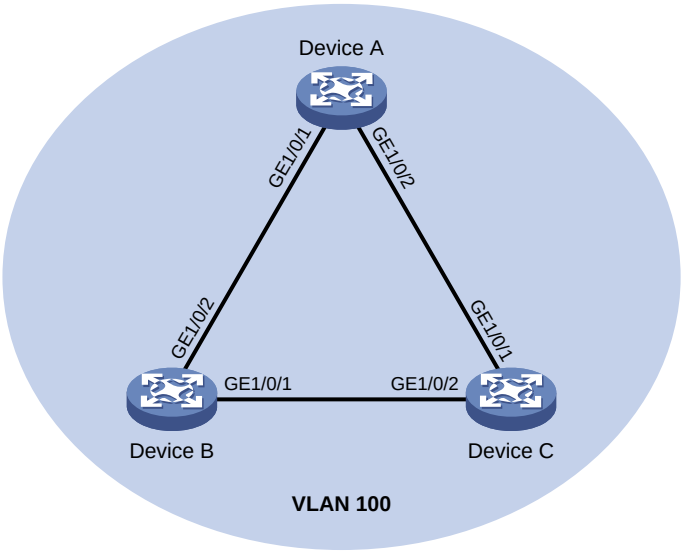
Task	Command
Display the loop detection configuration and status.	**display loopback-detection**

Loop detection configuration example

Network requirements

As shown in Figure 38, configure loop detection on Device A, so that Device A generates a log as a notification and automatically shuts down the port on which a loop is detected.

Figure 38 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLAN 100, and globally enable loop detection for the VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure the global loop protection action as shutdown.

```
[DeviceA] loopback-detection global action shutdown
```

Set the loop detection interval to 35 seconds.

```
[DeviceA] loopback-detection interval-time 35
```

2. Configure Device B:

Create VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB–vlan100] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configure Device C:

Create VLAN 100.

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC–vlan100] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/2] quit
```

Verifying the configuration

View the system logs on devices, for example, Device A.

```
[DeviceA]
%Feb 24 15:04:29:663 2013 DeviceA LPDT/4/LPDT_LOOPED: Loopback exists on
GigabitEthernet1/0/1.
%Feb 24 15:04:29:667 2013 DeviceA LPDT/4/LPDT_LOOPED: Loopback exists on
GigabitEthernet1/0/2.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT_RECOVERED: Loopback on GigabitEthernet1/0/1
recovered.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT_RECOVERED: Loopback on GigabitEthernet1/0/2
recovered.
```

The output shows the following information:

- Device A detected loops on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 within a loop detection interval.
- Loops on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 were removed.

Use the **display loopback-detection** command to display the loop detection configuration and status on devices, for example, Device A.

```
[DeviceA] display loopback-detection
Loop detection is enabled.
Loop detection interval is 35 second(s).
No loopback is detected.
```

The output shows that the device has removed the loops from GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 according to the shutdown action.

Display the status of GigabitEthernet 1/0/1 on devices, for example, Device A.

```
[DeviceA] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN (Loop detection down)
...
```

The output shows that GigabitEthernet 1/0/1 is already shut down by the loop detection module.

Display the status of GigabitEthernet 1/0/2 on Device A.

```
[DeviceA] display interface gigabitethernet 1/0/2
GigabitEthernet1/0/2 current state: DOWN (Loop detection down)
...
```

The output shows that GigabitEthernet 1/0/2 is already shut down by the loop detection module.

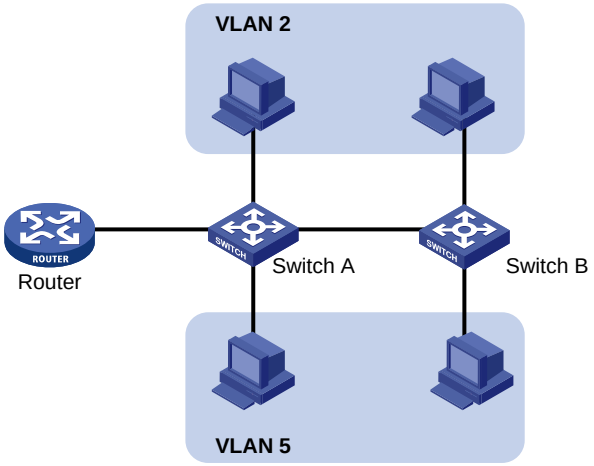
Configuring VLANs

Overview

Ethernet is a family of shared-media LAN technologies based on the CSMA/CD mechanism. An Ethernet LAN is both a collision domain and a broadcast domain. Because the medium is shared, collisions and broadcasts are common in an Ethernet LAN. Typically, bridges and Layer 2 switches can reduce collisions in an Ethernet LAN. To confine broadcasts, a Layer 2 switch must use the Virtual Local Area Network (VLAN) technology.

VLANs enable a Layer 2 switch to break a LAN down into smaller broadcast domains, as shown in Figure 39.

Figure 39 A VLAN diagram



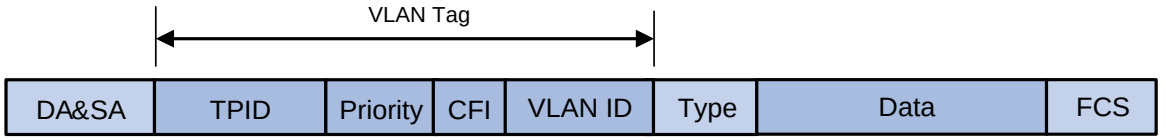
A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, you can assign all workstations and servers used by a particular workgroup to the same VLAN, regardless of their physical locations. Hosts in the same VLAN can directly communicate with one another. You need a router or a Layer 3 switch for hosts in different VLANs to communicate with one another.

All these VLAN features reduce bandwidth waste, improve LAN security, and enable flexible virtual group creation.

VLAN frame encapsulation

To identify Ethernet frames from different VLANs, IEEE 802.1Q inserts a four-byte VLAN tag between the destination and source MAC address (DA&SA) field and Type field.

Figure 40 VLAN tag placement and format



A VLAN tag includes the following fields:

- **TPID**—16-bit tag protocol identifier that indicates whether a frame is VLAN-tagged. By default, the TPID value 0x8100 identifies a VLAN-tagged frame. A device vendor can set TPID to

different values. For compatibility with a neighbor device, configure the TPID value on the device to be the same as the neighbor device.

- **Priority**—3-bit long, identifies the 802.1p priority of the frame. For more information, see *ACL and QoS Configuration Guide*.
- **CFI**—1-bit long canonical format indicator that indicates whether the MAC addresses are encapsulated in the standard format when packets are transmitted across different media. Available values include:
  - **0 (default)**—The MAC addresses are encapsulated in the standard format.
  - **1**—The MAC addresses are encapsulated in a nonstandard format.

  This field is always set to 0 for Ethernet.
- **VLAN ID**—12-bit long, identifies the VLAN to which the frame belongs. The VLAN ID range is 0 to 4095. VLAN IDs 0 and 4095 are reserved, and VLAN IDs 1 to 4094 are user configurable.

The way a network device handles an incoming frame depends on whether the frame has a VLAN-tag and the value of the VLAN tag (if any). For more information, see "Introduction."

Ethernet supports encapsulation formats Ethernet II, 802.3/802.2 LLC, 802.3/802.2 SNAP, and 802.3 raw. The Ethernet II encapsulation format is used here. For information about the VLAN tag fields in other frame encapsulation formats, see related protocols and standards.

For a frame with multiple VLAN tags, the device handles it according to its outer-most VLAN tag and transmits its inner VLAN tags as the payload.

Protocols and standards

IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*

Configuring basic VLAN settings

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Create a VLAN and enter its view, or create a list of VLANs.	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	By default, only the system default VLAN (VLAN 1) exists.
3. Enter VLAN view.	**vlan** *vlan-id*	To configure a VLAN after you create a list of VLANs, you must perform this step.
4. Configure a name for the VLAN.	**name** *text*	By default, VLAN names are in the format **VLAN** *vlan-id*. For example, the name of VLAN 100 is **VLAN 0100** by default.
5. Configure the description of the VLAN.	**description** *text*	The default setting is VLAN *vlan-id*, which is the ID of the VLAN. For example, the description of VLAN 100 is **VLAN 0100** by default.

NOTE:

- As the system default VLAN, VLAN 1 cannot be created or deleted.
- Before you delete a dynamic VLAN, a VLAN configured with the QoS policy, or a VLAN locked by an application, you must first remove the configuration from the VLAN.

Configuring basic settings of a VLAN interface

Hosts of different VLANs use VLAN interfaces to communicate at Layer 3. VLAN interfaces are virtual interfaces that do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface and assign an IP address to it. The VLAN interface acts as the gateway of the VLAN to forward packets destined for another IP subnet.

When you configure a VLAN interface, follow these restrictions and guidelines:

- Before you create a VLAN interface for a VLAN, create the VLAN first.
- You cannot create a VLAN interface for a sub-VLAN. For more information about sub-VLANs, see "Configuring super VLANs."
- You cannot create VLAN interfaces for secondary VLANs that have the following characteristics:
  - Associated with the same primary VLAN.
  - Enabled with Layer 3 communication in VLAN interface view of the primary VLAN interface.

  For more information about secondary VLANs, see "Configuring the private VLAN."

To configure basic settings of a VLAN interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VLAN interface and enter VLAN interface view.	**interface vlan-interface** *vlan-interface-id*	If the VLAN interface already exists, you enter its view directly. By default, no VLAN interface is created.
3. Assign an IP address to the VLAN interface.	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	By default, no IP address is assigned to any VLAN interface.
4. Configure the description of the VLAN interface.	**description** *text*	The default setting is the VLAN interface name. For example, **Vlan-interface1 Interface**.
5. (Optional.) Specify a member device for forwarding the traffic on the current VLAN interface.	**service slot** *slot-number*	By default, no member devices are specified.
6. Configure the MTU for the VLAN interface.	**mtu** *size*	The default setting is 1500 bytes.
7. Configure the expected bandwidth of the interface.	**bandwidth** *bandwidth-value*	By default, the expected bandwidth (in kbps) is the interface baud rate divided by 1000.
8. (Optional.) Restore the default settings for the VLAN interface.	**default**	N/A
9. (Optional.) Bring up the VLAN interface.	**undo shutdown**	By default, a VLAN interface is not manually shut down. The VLAN interface is up if one or more ports in the VLAN is up, and goes down if all ports in the VLAN go down.

Configuring port-based VLANs

Introduction

Port-based VLANs group VLAN members by port. A port forwards packets from a VLAN only after it is assigned to the VLAN.

Port link type

You can configure the link type of a port as access, trunk, or hybrid. The link types use the following VLAN tag handling methods:

- **Access**—An access port can forward packets from only one VLAN and send these packets untagged. An access port can connect a terminal device that does not support VLAN packets or is used in scenarios that do not distinguish VLANs.
- **Trunk**—A trunk port can forward packets from multiple VLANs. Except packets from the port VLAN ID (PVID), packets sent out of a trunk port are VLAN-tagged. Ports connecting network devices are typically configured as trunk ports.
- **Hybrid**—A hybrid port can forward packets from multiple VLANs. The tagging status of the packets forwarded by a hybrid port depends on the port configuration. Hybrid ports are typically used in one-to-two VLAN mapping to remove SVLAN tags for downlink traffic. For more information about one-to-two VLAN mapping, see "Configuring VLAN mapping."

PVID

The PVID identifies the default VLAN of a port.

When configuring the PVID on a port, follow these restrictions and guidelines:

- An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port.
- A trunk or hybrid port supports multiple VLANs and the PVID configuration.
- When you use the **undo vlan** command to delete the PVID of a port, either of the following events occurs depending on the port link type:
  - For an access port, the PVID of the port changes to VLAN 1.
  - For a hybrid or trunk port, the PVID setting on the port does not change.

  You can use a nonexistent VLAN as the PVID for a hybrid or trunk port, but not for an access port.
- As a best practice, set the same PVID for a local port and its peer.
- To prevent a port from dropping packets from its PVID and untagged packets, assign the port to its PVID.

How ports of different link types handle frames

Actions	Access	Trunk	Hybrid
In the inbound direction for an untagged frame	Tags the frame with the PVID tag.	• If the PVID is permitted on the port, tags the frame with the PVID tag. • If not, drops the frame.	
In the inbound direction for a tagged frame	• Receives the frame if its VLAN ID is the same as the PVID. • Drops the frame if its VLAN ID is different from the	• Receives the frame if its VLAN is permitted on the port. • Drops the frame if its VLAN is not permitted on the port.	

Actions	Access	Trunk	Hybrid
	PVID.		
In the outbound direction	Removes the VLAN tag and sends the frame.	• Removes the tag and sends the frame if the frame carries the PVID tag and the port belongs to the PVID. • Sends the frame without removing the tag if its VLAN is carried on the port but is different from the PVID.	Sends the frame if its VLAN is permitted on the port. The tagging status of the frame depends on the **port hybrid vlan** command configuration.

In a VLAN-aware network, the default processing order for untagged packets is as follows, in descending order of priority:

- MAC-based VLANs.
- IP subnet-based VLANs.
- Protocol-based VLANs.
- Port-based VLANs.

Assigning an access port to a VLAN

You can assign an access port to a VLAN in VLAN view or interface view.

Make sure the VLAN has been created.

Assigning one or multiple access ports to a VLAN in VLAN view

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Assign one or a group of access ports to the VLAN.	**port** *interface-list*	By default, all ports belong to VLAN 1.

Assigning an access port to a VLAN in interface view

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	• The configuration made in Layer 2 Ethernet interface view applies only to the port. • The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports. If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port. If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.

Step	Command	Remarks
3. Configure the link type of the port as access.	**port link-type access**	By default, all ports are access ports.
4. (Optional.) Assign the access port to a VLAN.	**port access vlan** *vlan-id*	By default, all access ports belong to VLAN 1.

Assigning a trunk port to a VLAN

A trunk port supports multiple VLANs. You can assign it to a VLAN in interface view.

When you assign a trunk port to a VLAN, follow these restrictions and guidelines:

- To change the link type of a port from trunk to hybrid or vice versa, set the link type to access first.
- To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

To assign a trunk port to one or multiple VLANs:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	• The configuration made in Layer 2 Ethernet interface view applies only to the port. • The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports. If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port. If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
3. Configure the link type of the port as trunk.	**port link-type trunk**	By default, all ports are access ports.
4. Assign the trunk port to the specified VLANs.	**port trunk permit vlan** { *vlan-id-list* | **all** }	By default, a trunk port permits only VLAN 1.
5. (Optional.) Configure the PVID of the trunk port.	**port trunk pvid vlan** *vlan-id*	The default setting is VLAN 1.

Assigning a hybrid port to a VLAN

A hybrid port supports multiple VLANs. You can assign it to the specified VLANs in interface view. Make sure the VLANs have been created.

When you assign a hybrid port to a VLAN, follow these restrictions and guidelines:

- To change the link type of a port from trunk to hybrid or vice versa, set the link type to access first.

- To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

To assign a hybrid port to one or multiple VLANs:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	• The configuration made in Layer 2 Ethernet interface view applies only to the port. • The configuration made in Layer 2 aggregate interface view applies to the aggregate interface and its aggregation member ports. If the system fails to apply the configuration to an aggregation member port, it skips the port and moves to the next member port. If the system fails to apply the configuration to the aggregate interface, it stops applying the configuration to aggregation member ports.
3. Configure the link type of the port as hybrid.	**port link-type hybrid**	By default, all ports are access ports.
4. Assign the hybrid port to the specified VLANs.	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
5. (Optional.) Configure the PVID of the hybrid port.	**port hybrid pvid vlan** *vlan-id*	By default, the PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Configuring MAC-based VLANs

Introduction

This feature is available only on hybrid ports.

The MAC-based VLAN feature assigns hosts to a VLAN based on their MAC addresses. This feature is usually used with security technologies such as 802.1X to provide secure and flexible network access for terminal devices.

Static MAC-based VLAN assignment

Use static MAC-based VLAN assignment in networks that have a small number of VLAN users. To configure static MAC-based VLAN assignment on a port, perform the following tasks:

1. Create MAC-to-VLAN entries.
2. Enable the MAC-based VLAN feature on the port.
3. Assign the port to the MAC-based VLAN.

A port configured with static MAC-based VLAN assignment processes a received frame as follows before sending the frame out:

- For an untagged frame, the port determines its VLAN ID in the following workflow:
  a. The port first performs a fuzzy match as follows:
    - Searches for the MAC-to-VLAN entries whose masks are not all-Fs.
    - Performs a logical AND operation on the source MAC address and each of these masks.

      If the result of an AND operation matches the MAC address in a MAC-to-VLAN entry, the port tags the frame with the VLAN ID specific to this entry.

  b. If the fuzzy match fails, the port performs an exact match. It searches for MAC-to-VLAN entries whose masks are all-Fs. If the source MAC address of the frame matches the MAC address of a MAC-to-VLAN entry, the port tags the frame with the VLAN ID specific to this entry.

  c. If no matching VLAN ID is found, other criteria, such as IP subnet or protocol, are used for VLAN assignment.

  d. If no VLAN is available, the port tags the frame with its PVID.
- For a tagged frame, the port determines whether the VLAN ID of the frame is permitted on the port.
  - If the VLAN ID of the frame is permitted on the port, the port forwards the frame.
  - If the VLAN ID of the frame is not permitted on the port, the port drops the frame.

Dynamic MAC-based VLAN assignment

When you cannot determine the target MAC-based VLANs of a port, you can use dynamic MAC-based VLAN assignment on the port. To use dynamic MAC-based VLAN assignment, perform the following tasks:

1. Create MAC-to-VLAN entries.
2. Enable the MAC-based VLAN feature on the port.
3. Enable dynamic MAC-based VLAN assignment on the port.

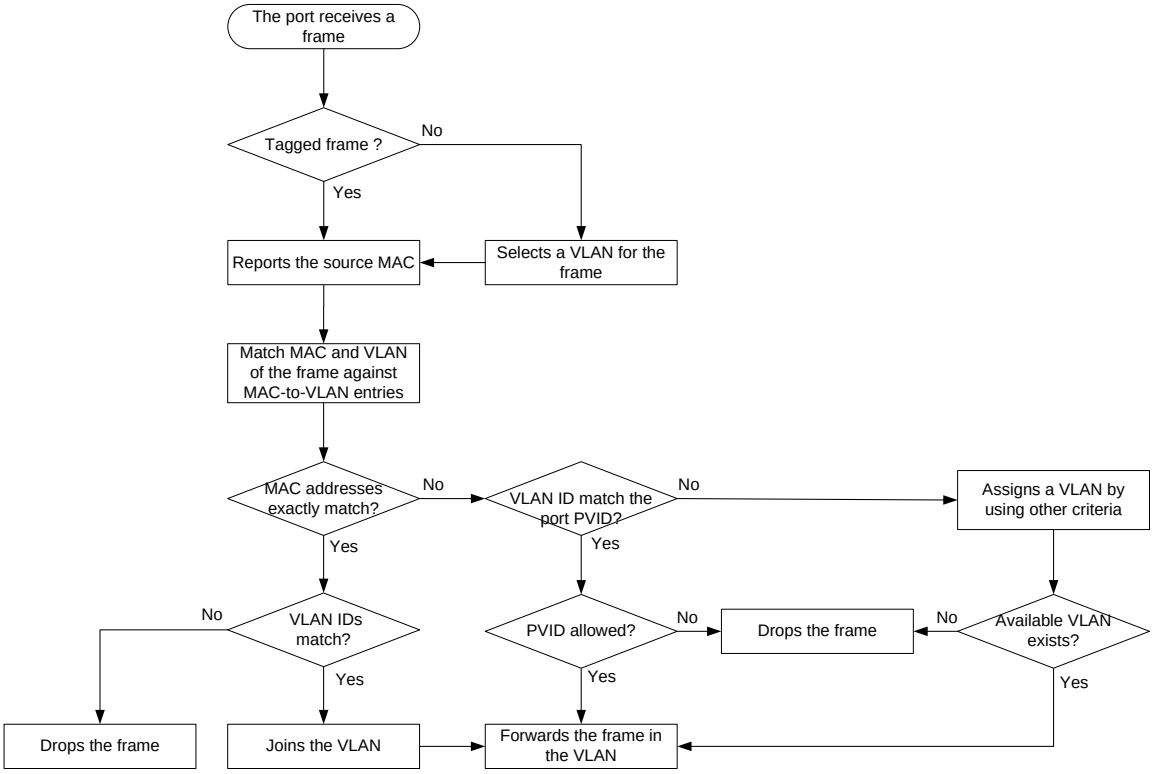
Dynamic MAC-based VLAN assignment uses the following workflow, as shown in Figure 41:

1. When a port receives a frame, it first determines whether the frame is tagged.
   - If the frame is tagged, the port reports the source MAC address of the frame.
   - If the frame is untagged, the port selects a VLAN for the frame by using the following matching order:
     - MAC-based VLAN.
     - IP subnet-based VLAN.
     - Protocol-based VLAN.
     - Port-based VLAN.

     After tagging the frame with the selected VLAN, the port reports the source MAC address of the frame.
2. The port uses the source address and VLAN of the frame to match the MAC-to VLAN entries.
   - If the source MAC address of the frame exactly matches the MAC address in a MAC-to-VLAN entry, the port checks whether the VLAN ID of the frame matches the VLAN in the entry.
     - If the two VLAN IDs match, the port joins the VLAN and forwards the frame.
     - If the two VLAN IDs do not match, the port drops the frame.
   - If the source MAC address of the frame does not match any MAC addresses in MAC-to-VLAN entries exactly, the port checks whether the VLAN ID of the frame is its PVID.
     - If the VLAN ID of the frame is the PVID of the port, the port determines whether it allows the PVID. If the PVID is allowed, the port forwards the frame within the PVID. If the PVID is not allowed, the port drops the frame.

– If the VLAN ID of the frame is not the PVID of the port, the port matches the VLAN ID of the frame by using other criteria, such as IP subnet or protocol, and forwards the frame. If no VLAN is available, the port drops the frame.

Figure 41 Flowchart for processing a frame in dynamic MAC-based VLAN assignment



When you configure dynamic MAC-based VLAN assignment, follow these guidelines:

- When a port joins a VLAN specified in the MAC-to-VLAN entry, one of the following events occurs depending on the port configuration:
  - If the port has not been configured to allow packets from the VLAN to pass through, the port joins the VLAN as an untagged member.
  - If the port has been configured to allow packets from the VLAN to pass through, the port configuration remains the same.
- If you configure both static and dynamic MAC-based VLAN assignments on a port, dynamic MAC-based VLAN assignment takes effect.
- When a packet matches a MAC-to-VLAN entry, the device determines a forwarding policy for the packet according to the 802.1p priority of the VLAN in the MAC-to-VLAN entry.

Server-assigned MAC-based VLAN

Use the server-assigned MAC-based VLAN feature with access authentication, such as MAC-based 802.1X authentication, to implement secure and flexible terminal access. In addition to configuring the server-assigned MAC-based VLAN feature on the device, you must configure the username-to-VLAN entries on the access authentication server.

When a user passes authentication of the access authentication server, the server issues the VLAN ID for the user to the device. The device then performs the following operations:

1. Generates a MAC-to-VLAN entry by using the source MAC address of the user packet and the received VLAN ID. The VLAN is a MAC-based VLAN.
2. Assigns the port that connects the user to the MAC-based VLAN.

When the user goes offline, the device automatically deletes the MAC-to-VLAN entry and removes the port from the MAC-based VLAN. For more information about 802.1X and MAC authentication, see *Security Configuration Guide*.

Configuration restrictions and guidelines

When you configure MAC-based VLANs, follow these restrictions and guideline:

- Do not configure a VLAN as both a super VLAN and a MAC-based VLAN.
- As a best practice, do not use dynamic MAC-based VLAN assignment together with the MAC learning limit or disabling MAC address learning.

  When dynamic MAC-based VLAN assignment is enabled on a port, packets received on the port are delivered to the CPU. Processing to these packets has the highest priority. The configuration of MAC learning limit and disabling of MAC address learning cannot take effect.
- Do not use dynamic MAC-based VLAN assignment together with 802.1X or MAC authentication.
- For successful dynamic MAC-based VLAN assignment, use static VLANs when you create MAC-to-VLAN entries.
- The MAC-based VLAN feature is mainly configured on downlink ports of user access devices. Do not enable this function with link aggregation.
- As a best practice, do not use dynamic MAC-based VLAN assignment together with MSTP. In MSTP mode, if a port is blocked in the MSTI of the target VLAN, the port drops the received packets instead of delivering them to the CPU. As a result, the receiving port will not be dynamically assigned to the VLAN.
- As a best practice, do not use dynamic MAC-based VLAN assignment together with PVST. In PVST mode, if the target VLAN is not permitted on a port, the port is placed in blocked state. The received packets are dropped instead of being delivered to the CPU. As a result, the receiving port will not be dynamically assigned to the VLAN.
- As a best practice, do not configure both dynamic MAC-based VLAN assignment and automatic voice VLAN assignment mode on a port. If you have to configure both of them on a port, configure dynamic MAC-based VLAN assignment first. If you configure them in a reverse order, conflict will occur. When you remove one of the configurations, the operation of the other is affected.

Configuring static MAC-based VLAN assignment

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a MAC-to-VLAN entry.	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]	N/A
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the link type of the port as hybrid.	**port link-type hybrid**	By default, all ports are access ports.
5. Configure the hybrid port to forward packets from the MAC-based VLANs.	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
6. Enable the MAC-based VLAN feature.	**mac-vlan enable**	By default, this feature is disabled.

Step	Command	Remarks
7. (Optional.) Configure VLAN matching order.	**vlan precedence** { **mac-vlan** | **ip-subnet-vlan** }	By default, the system assigns VLANs based on the MAC address preferentially.

Configuring dynamic MAC-based VLAN assignment

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a MAC-to-VLAN entry.	**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**dot1q** *priority*]	The VLAN assignment for a port is triggered only when the source MAC address of its receiving packet exactly matches the MAC address in the MAC-to-VLAN entry.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the link type of the port as hybrid.	**port link-type hybrid**	By default, all ports are access ports.
5. Enable the MAC-based VLAN feature.	**mac-vlan enable**	By default, MAC-based VLAN is disabled.
6. Enable dynamic MAC-based VLAN assignment.	**mac-vlan trigger enable**	By default, dynamic MAC-based VLAN assignment is disabled.
7. (Optional.) Configure VLAN matching order.	**vlan precedence** { **mac-vlan** | **ip-subnet-vlan** }	By default, the system assigns VLANs based on the MAC address preferentially. When you enable dynamic MAC-based VLAN assignment, configure the **vlan precedence mac-vlan** command as a best practice to ensure the priority of MAC-based VLAN matching. If you execute the **vlan precedence ip-subnet-vlan** command, the command will not take effect.
8. (Optional.) Disable the port from forwarding packets that fail the exact MAC address match in its PVID.	**port pvid forbidden**	By default, when a port receives packets whose source MAC addresses fail the exact match, the port forwards them in its PVID.

Configuring server-assigned MAC-based VLAN

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the link type of the ports as hybrid.	**port link-type hybrid**	By default, all ports are access ports.
4. Configure the hybrid port to forward packets from the MAC-based VLANs.	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
5. Enable the MAC-based VLAN feature.	**mac-vlan enable**	By default, MAC-based VLAN is disabled.
6. Configure 802.1X or MAC authentication.	For more information, see *Security Command Reference*.	N/A

Configuring IP subnet-based VLANs

In this method, packets are assigned to VLANs based on their source IP addresses and subnet masks. A port configured with IP subnet-based VLANs assigns a received untagged packet to a VLAN based on the source address of the packet.

Use this feature when packets from an IP subnet or IP address must be transmitted in a VLAN.

This feature is available only on hybrid ports, and it processes only untagged packets.

An IP subnet-based VLAN has one or multiple subnets to match inbound packets. Each subnet has a unique index in the IP subnet-based VLAN. All subnets in an IP subnet-based VLAN have the same VLAN ID.

To configure a IP subnet-based VLAN:

Task	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Associate an IP subnet or IP address with the VLAN.	**ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* [*mask*]	By default, a VLAN is not associated with any IP subnets or IP addresses. A multicast subnet or a multicast address cannot be associated with a VLAN.
4. Return to system view.	**quit**	N/A
5. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	• The configurations made in Layer 2 Ethernet interface view apply only to the port. • The configurations made in Layer 2 aggregate interface view apply to the aggregate interface and its aggregation member ports. If the system fails to apply the

Task	Command	Remarks
		configurations to the aggregate interface, it stops applying the configurations to the aggregation member ports. If the system fails to apply the configurations to an aggregation member port, it skips the port and moves to the next member port.
6. Configure the port link type as hybrid.	**port link-type hybrid**	By default, all ports are access ports.
7. Assign the hybrid port to the specified IP subnet-based VLANs.	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
8. Associate the hybrid port with the specified IP subnet-based VLAN.	**port hybrid ip-subnet-vlan vlan** *vlan-id*	By default, no IP subnet-based VLAN is associated with a hybrid port.

Configuring protocol-based VLANs

The protocol-based VLAN feature assigns inbound packets to different VLANs based on their protocol types and encapsulation formats. The protocols available for VLAN assignment include IP, IPX, and AT. The encapsulation formats include Ethernet II, 802.3 raw, 802.2 LLC, and 802.2 SNAP.

A protocol template defines a protocol type and an encapsulation format. A combination of a protocol-based VLAN ID and a protocol index uniquely identify a protocol template. You can assign multiple protocol templates to a protocol-based VLAN.

This feature is available only on hybrid ports, and it processes only untagged packets. It associates the available network service types with VLANs and facilitates network management and maintenance.

A protocol-based VLAN has one or multiple protocol templates. A protocol template defines a protocol type and an encapsulation format as the match criteria to match inbound packets. Each protocol template has a unique index in the protocol-based VLAN. All protocol templates in a protocol-based VLAN have the same VLAN ID.

For a port to assign inbound packets to protocol-based VLANs, perform the following tasks:

- Assign the port to the protocol-based VLANs.
- Associate the port with the protocol templates of the protocol-based VLANs.

When an untagged packet arrives at the port, the port processes the packet as follows:

- If the protocol type and encapsulation format in the packet match a protocol template, the port tags the packet with the VLAN tag specific to the protocol template.
- If no protocol templates are matched, the port tags the packet with its PVID.

The voice VLAN in automatic mode processes only tagged voice traffic. Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN.

To configure a protocol-based VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter VLAN view.	**vlan** *vlan-id*	If the specified VLAN does not exist, this command first creates the VLAN and enters VLAN view of this VLAN.
3. Create a protocol template for the VLAN.	**protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }	By default, no protocol template is configured for a VLAN.
4. Exit VLAN view.	**quit**	N/A
5. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	• The configurations made in Layer 2 Ethernet interface view apply only to the port. • The configurations made in Layer 2 aggregate interface view apply to the aggregate interface and its aggregation member ports. If the system fails to apply the configurations to the aggregate interface, it stops applying the configurations to aggregation member ports. If the system fails to apply the configurations to an aggregation member port, it skips the port and moves to the next member port.
6. Configure the port link type as hybrid.	**port link-type hybrid**	By default, all ports are access ports.
7. Assign the hybrid port to the specified protocol-based VLANs.	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
8. Associate the hybrid port with the specified protocol-based VLAN.	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	By default, a port is not associated with any protocol-based VLANs.

Configuring a VLAN group

After you configure a VLAN group on the device, the authentication sever can assign the VLAN group name to the 802.1X user that passes authentication. The VLAN group name identifies this group of VLANs. For more information about 802.1X authentication, see *Security Configuration Guide*.

To configure a VLAN group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VLAN group and enter VLAN group view.	**vlan-group** *group-name*	By default, no VLAN group exists.
3. Add VLANs to the VLAN group.	**vlan-list** *vlan-id-list*	By default, no VLAN exists in a VLAN group.

Displaying and maintaining VLANs

Execute **display** commands in any view.

Task	Command
Display VLAN interface information.	**display interface vlan-interface** [*interface-number*] [**brief** [**description** | **down**]]
Display MAC-to-VLAN entries.	**display mac-vlan { all | dynamic | mac-address** *mac-address* [**mask** *mac-mask*] **| static | vlan** *vlan-id* **}**
Display all ports that are enabled with the MAC-based VLAN feature.	**display mac-vlan interface**
Display information about IP subnet-based VLANs that are associated with the specified ports.	**display ip-subnet-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
Display information about IP subnet-based VLANs.	**display ip-subnet-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
Display information about protocol-based VLANs that are associated with the specified ports.	**display protocol-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
Display information about protocol-based VLANs.	**display protocol-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
Display VLAN information.	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]
Display brief VLAN information.	**display vlan brief**
Display VLAN group information.	**display vlan-group** [*group-name*]
Display hybrid ports or trunk ports on the device.	**display port** { **hybrid** | **trunk** }

VLAN configuration examples

Port-based VLAN configuration example

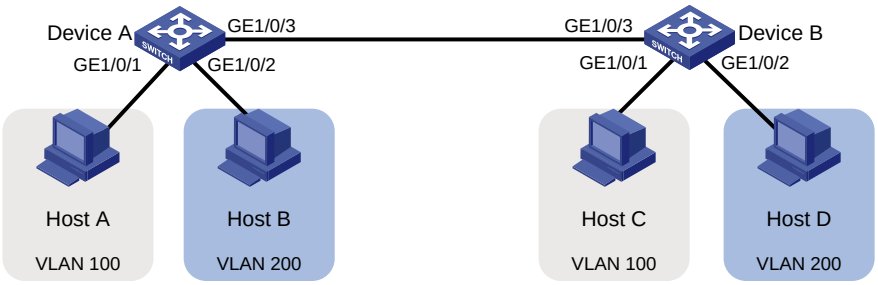
Network requirements

As shown in Figure 42:

- Host A and Host C belong to Department A. VLAN 100 is assigned to Department A.
- Host B and Host D belong to Department B. VLAN 200 is assigned to Department B.

Configure port-based VLANs so that only hosts in the same department can communicate with each other.

Figure 42 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLAN 100, and assign GigabitEthernet 1/0/1 to VLAN 100.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] port gigabitethernet 1/0/1
   [DeviceA-vlan100] quit
   ```

   # Create VLAN 200, and assign GigabitEthernet 1/0/2 to VLAN 200.

   ```
   [DeviceA] vlan 200
   [DeviceA-vlan200] port gigabitethernet 1/0/2
   [DeviceA-vlan200] quit
   ```

   # Configure GigabitEthernet 1/0/3 as a trunk port to forward packets from VLANs 100 and 200 to Device B.

   ```
   [DeviceA] interface gigabitethernet 1/0/3
   [DeviceA-GigabitEthernet1/0/3] port link-type trunk
   [DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
   Please wait... Done.
   ```

2. Configure Device B in the same way Device A is configured. (Details not shown.)
3. Configure hosts:
   - Configure Host A and Host C to be on the same IP subnet. For example, 192.168.100.0/24.
   - Configure Host B and Host D to be on the same IP subnet. For example, 192.168.200.0/24.

Verifying the configuration

Verify that Host A and Host C can ping each other, but they both fail to ping Host B. (Details not shown.)

Verify that Host B and Host D can ping each other, but they both fail to ping Host A. (Details not shown.)

Verify that VLANs 100 and 200 are correctly configured on devices, for example, on Device A.

```
[DeviceA-GigabitEthernet1/0/3] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports:
    GigabitEthernet1/0/1
```

```
[DeviceA-GigabitEthernet1/0/3] display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports:
    GigabitEthernet1/0/2
```

MAC-based VLAN configuration example

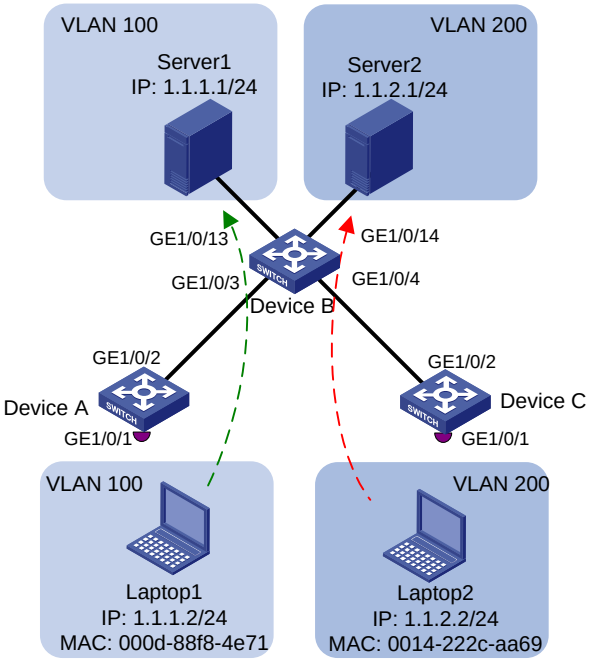
Network requirements

As shown in Figure 43:

- GigabitEthernet 1/0/1 of Device A and Device C are each connected to a meeting room. Laptop 1 and Laptop 2 are used for meetings and might be used in either of the two meeting rooms.
- Different departments own Laptop 1 and Laptop 2. The two departments use VLANs 100 and 200, respectively.

Configure MAC-based VLANs, so that each laptop is able to access only its own department server, no matter which meeting room they are used in.

Figure 43 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLANs 100 and 200.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] quit
   ```

```
[DeviceA] vlan 200
[DeviceA-vlan200] quit
```

Associate the MAC addresses of Laptop 1 and Laptop 2 with VLANs 100 and 200, respectively.

```
[DeviceA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[DeviceA] mac-vlan mac-address 0014-222c-aa69 vlan 200
```

Configure GigabitEthernet 1/0/1 as a hybrid port to forward packets from VLANs 100 and 200 without VLAN tags.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Enable the MAC-based VLAN feature on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] mac-vlan enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure the uplink port GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 200.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceA-GigabitEthernet1/0/2] quit
```

2. Configure Device B:

Create VLAN 100 and assign GigabitEthernet 1/0/13 to VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/13
[DeviceB-vlan100] quit
```

Create VLAN 200 and assign GigabitEthernet 1/0/14 to VLAN 200.

```
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/14
[DeviceB-vlan200] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign the port to VLANs 100 and 200.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/4 as a trunk port, and assign the port to VLANs 100 and 200.

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/4] quit
```

3. Configure Device C in the same way as the Device A is configured. (Details not shown.)

Verifying the configuration

Verify that Laptop 1 can access only Server 1, and Laptop 2 can access only Server 2. (Details not shown.)

Verify the MAC-to-VLAN entries on Device A and Device C, for example, Device A.

```
[DeviceA] display mac-vlan all
  The following MAC VLAN addresses exist:
```

```
S:Static  D:Dynamic
MAC address      Mask             VLAN ID  Dot1q      State
000d-88f8-4e71   ffff-ffff-ffff   100       0          S
0014-222c-aa69   ffff-ffff-ffff   200       0          S

Total MAC VLAN address count: 2
```

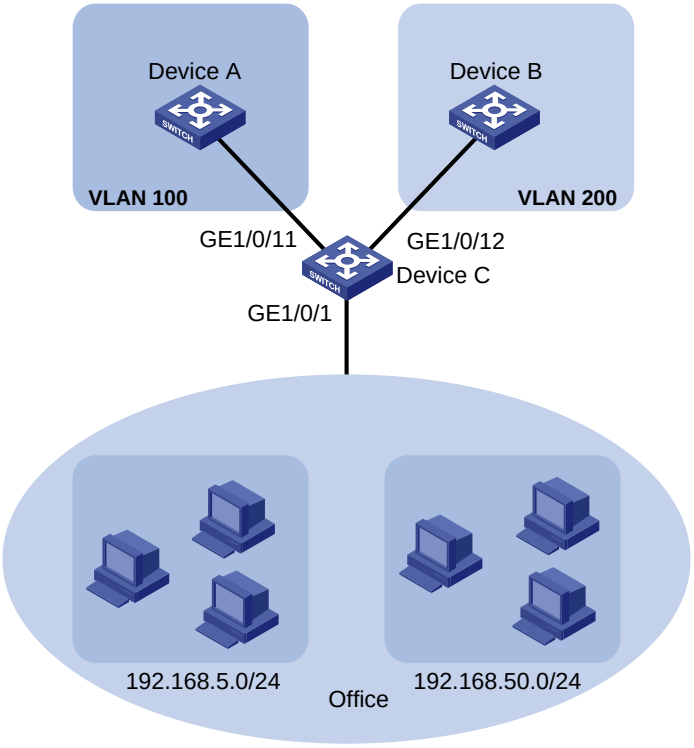
IP subnet-based VLAN configuration example

Network requirements

As shown in Figure 44, the hosts in the office belong to different IP subnets.

Configure Device C to transmit packets from 192.168.5.0/24 and 192.168.50.0/24 in VLANs 100 and 200, respectively.

Figure 44 Network diagram



Configuration procedure

1. Configure Device C:

   # Associate IP subnet 192.168.5.0/24 with VLAN 100.

   ```
   <DeviceC> system-view
   [DeviceC] vlan 100
   [DeviceC-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
   [DeviceC-vlan100] quit
   ```

   # Associate IP subnet 192.168.50.0/24 with VLAN 200.

   ```
   [DeviceC] vlan 200
   [DeviceC-vlan200] ip-subnet-vlan ip 192.168.50.0 255.255.255.0
   [DeviceC-vlan200] quit
   ```

Configure GigabitEthernet 1/0/11 as a hybrid port, and assign it to VLAN 100 as a tagged VLAN member.

```
[DeviceC] interface gigabitethernet 1/0/11
[DeviceC-GigabitEthernet1/0/11] port link-type hybrid
[DeviceC-GigabitEthernet1/0/11] port hybrid vlan 100 tagged
[DeviceC-GigabitEthernet1/0/11] quit
```

Configure GigabitEthernet1/0/12 as a hybrid port, and assign it to VLAN 200 as a tagged VLAN member.

```
[DeviceC] interface gigabitethernet 1/0/12
[DeviceC-GigabitEthernet1/0/12] port link-type hybrid
[DeviceC-GigabitEthernet1/0/12] port hybrid vlan 200 tagged
[DeviceC-GigabitEthernet1/0/12] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type hybrid
[DeviceC-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Associate GigabitEthernet 1/0/1 with IP subnet-based VLANs 100 and 200.

```
[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
[DeviceC-GigabitEthernet1/0/1] quit
```

2. Configure Device A and Device B to forward packets from VLANs 100 and 200, respectively. (Details not shown.)

Verifying the configuration

Display information about all IP subnet-based VLANs.

```
[DeviceC] display ip-subnet-vlan vlan all
 VLAN ID: 100
  Subnet index      IP address      Subnet mask
  0                 192.168.5.0     255.255.255.0

 VLAN ID: 200
  Subnet index      IP address      Subnet mask
  0                 192.168.50.0    255.255.255.0
```

Display IP subnet-based VLANs on GigabitEthernet 1/0/1.

```
[DeviceC] display ip-subnet-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet index    IP address       Subnet mask       Status
  100       0               192.168.5.0      255.255.255.0     Active
  200       0               192.168.50.0     255.255.255.0     Active
```

Protocol-based VLAN configuration example

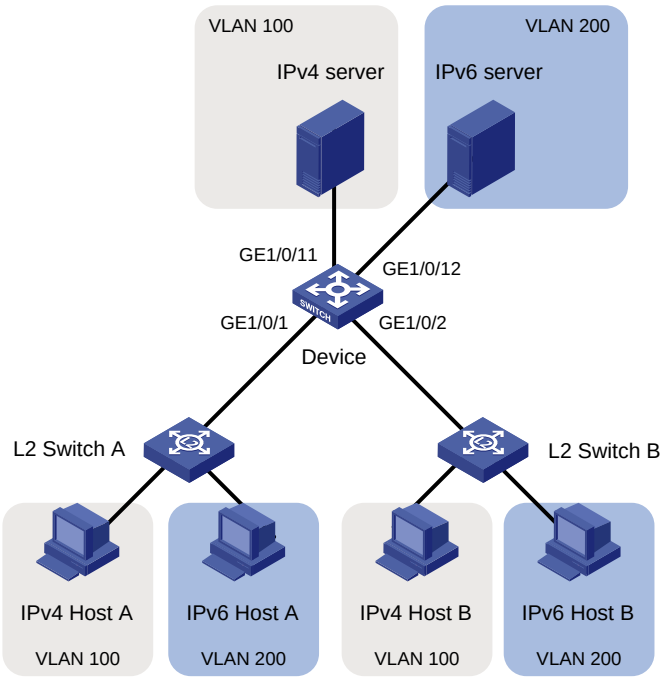
Network requirements

As shown in Figure 45:

- The majority of hosts in a lab environment run the IPv4 protocol.
- The other hosts run the IPv6 protocol for teaching purposes.

To isolate IPv4 and IPv6 traffic at Layer 2, configure protocol-based VLANs to associate the IPv4 and ARP protocols with VLAN 100, and associate the IPv6 protocol with VLAN 200.

Figure 45 Network diagram



Configuration procedure

In this example, L2 Switch A and L2 Switch B use the factory configuration.

1. Configure Device:

   # Create VLAN 100, and configure the description for VLAN 100 as **protocol VLAN for IPv4**.

   ```
   <Device> system-view
   [Device] vlan 100
   [Device-vlan100] description protocol VLAN for IPv4
   ```

   # Assign GigabitEthernet 1/0/11 to VLAN 100.

   ```
   [Device-vlan100] port gigabitethernet 1/0/11
   [Device-vlan100] quit
   ```

   # Create VLAN 200, and configure the description for VLAN 200 as **protocol VLAN for IPv6**.

   ```
   [Device] vlan 200
   [Device-vlan200] description protocol VLAN for IPv6
   ```

   # Assign GigabitEthernet 1/0/12 to VLAN 200.

   ```
   [Device-vlan200] port gigabitethernet 1/0/12
   ```

   # Configure VLAN 200 as a protocol-based VLAN, and create an IPv6 protocol template with the index 1 for VLAN 200.

   ```
   [Device-vlan200] protocol-vlan 1 ipv6
   [Device-vlan200] quit
   ```

   # Configure VLAN 100 as a protocol-based VLAN, and create an IPv4 protocol template with the index 1 for VLAN 100.

   ```
   [Device] vlan 100
   [Device-vlan100] protocol-vlan 1 ipv4
   ```

   # Create an ARP protocol template with the index 2 for VLAN 100. (In Ethernet II encapsulation, the protocol type ID for ARP is 0x0806.)

```
[Device-vlan100] protocol-vlan 2 mode ethernetii etype 0806
[Device-vlan100] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type hybrid
[Device-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Associate GigabitEthernet 1/0/1 with the IPv4 and ARP protocol templates of VLAN 100 and the IPv6 protocol template of VLAN 200.

```
[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 1 to 2
[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 1
[Device-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-type hybrid
[Device-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
```

Associate GigabitEthernet 1/0/2 with the IPv4 and ARP protocol templates of VLAN 100 and the IPv6 protocol template of VLAN 200.

```
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1 to 2
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1
[Device-GigabitEthernet1/0/2] quit
```

2. Configure hosts and servers:

a. Configure IPv4 Host A, IPv4 Host B, and IPv4 server to be on the same network segment (192.168.100.0/24, for example). (Details not shown.)

b. Configure IPv6 Host A, IPv6 Host B, and IPv6 server to be on the same network segment (2001::1/64, for example). (Details not shown.)

Verifying the configuration

1. Verify the following:

- The hosts and the server in VLAN 100 can successfully ping one another. (Details not shown.)
- The hosts and the server in VLAN 200 can successfully ping one another. (Details not shown.)
- The hosts or the server in VLAN 100 cannot ping the hosts or server in VLAN 200. (Details not shown.)

2. Verify the protocol-based VLAN configuration:

Display protocol-based VLANs on Device.

```
[Device] display protocol-vlan vlan all
 VLAN ID: 100
  Protocol index  Protocol type
  1               IPv4
  2               Ethernet II Etype 0x0806

 VLAN ID: 200
  Protocol index  Protocol type
  1               IPv6
```

Display protocol-based VLANs on the ports of Device.

```
[Device] display protocol-vlan interface all
```

```
Interface: GigabitEthernet1/0/1
 VLAN ID  Protocol index  Protocol type             Status
 100      1               IPv4                      Active
 100      2               Ethernet II Etype 0x0806  Active
 200      1               IPv6                      Active

Interface: GigabitEthernet 1/0/2
 VLAN ID  Protocol index  Protocol type             Status
 100      1               IPv4                      Active
 100      2               Ethernet II Etype 0x0806  Active
 200      1               IPv6                      Active
```

Configuring super VLANs

Hosts in a VLAN typically use IP addresses in the same subnet. For Layer 3 interoperability with other VLANs, you can create a VLAN interface for the VLAN and assign an IP address to it. This requires a large number of IP addresses.

The super VLAN feature was introduced to save IP addresses. A super VLAN is associated with multiple sub-VLANs. These sub-VLANs use the VLAN interface of the super VLAN (also known as a super VLAN interface) as the gateway for Layer 3 communication.

You can create a VLAN interface for a super VLAN and assign an IP address to it. However, you cannot create a VLAN interface for a sub-VLAN. You can assign a physical port to a sub-VLAN, but you cannot assign a physical port to a super VLAN. Sub-VLANs are isolated at Layer 2.

You can enable Layer 3 communication between sub-VLANs by performing the following tasks:

1. Create a super VLAN and the super VLAN interface.
2. Enable local proxy ARP or ND on the super VLAN interface as follows:
   - In an IPv4 network, enable local proxy ARP on the super VLAN interface. The super VLAN can then process ARP requests and replies sent from the sub-VLANs.
   - In an IPv6 network, enable local proxy ND on the super VLAN interface. The super VLAN can forward and process the NS and NA messages sent from the sub-VLANs.

Super VLAN configuration task list

Tasks at a glance
(Required.) Creating a sub-VLAN
(Required.) Configuring a super VLAN
(Required.) Configuring a super VLAN interface

Creating a sub-VLAN

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a sub-VLAN.	**vlan** *vlan-id*	By default, only the system default VLAN (VLAN 1) exists.

Configuring a super VLAN

When you configure a super VLAN, follow these restrictions and guidelines:

- Do not configure a VLAN as both a super VLAN and a guest VLAN, Auth-Fail VLAN, or critical VLAN for a port, and vice versa. For more information about guest VLANs, Auth-Fail VLANs, and critical VLANs, see *Security Configuration Guide*.
- Do not configure a VLAN as both a super VLAN and a MAC-based VLAN.
- Do not configure a VLAN as both a super VLAN and a sub-VLAN.
- You can configure Layer 2 multicast for super VLANs. However, the configuration does not take effect because super VLANs do not have physical ports.

To configure a super VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Configure the VLAN as a super VLAN.	**supervlan**	By default, a VLAN is not a super VLAN.
4. Associate the super VLAN with the sub-VLANs.	**subvlan** *vlan-id-list*	By default, a super VLAN is not associated with any sub-VLANs. Make sure the sub-VLANs already exist before associating them with a super VLAN.

Configuring a super VLAN interface

As a best practice, do not configure VRRP for the VLAN interface of a super VLAN because the configuration affects network performance. For more information about VRRP, see *High Availability Configuration Guide*.

To configure a super VLAN interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VLAN interface and enter its view.	**interface vlan-interface** *vlan-interface-id*	The *vlan-interface-id* argument must be the super VLAN ID.
3. Configure an IP address for the VLAN interface of the super VLAN.	• Configure an IPv4 address: **ip address** *ip-address* { *mask-length* | *mask* } [**sub**] • Configure an IPv6 address: **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }	By default, no IP address is configured for a VLAN interface.
4. (Optional.) Configure Layer 3 communication between sub-VLANs.	• Enable local proxy ARP for devices that run IPv4 protocols: **local-proxy-arp enable** • Enable local proxy ND for devices that run IPv6 protocols: **local-proxy-nd enable**	By default: • Sub-VLANs cannot communicate with each other at Layer 3. • Local proxy ARP or ND is disabled. For more information about local proxy ARP and proxy ND, see *Layer 3—IP Services Configuration Guide*. For more information about **local-proxy-arp enable** and **local-proxy-nd enable** commands, see *Layer 3—IP Services Command Reference*.

Displaying and maintaining super VLANs

Execute **display** commands in any view.

Task	Command
Display information about super VLANs and all sub-VLANs associated with each super VLAN.	**display supervlan** [*supervlan-id*]

Super VLAN configuration example

Network requirements

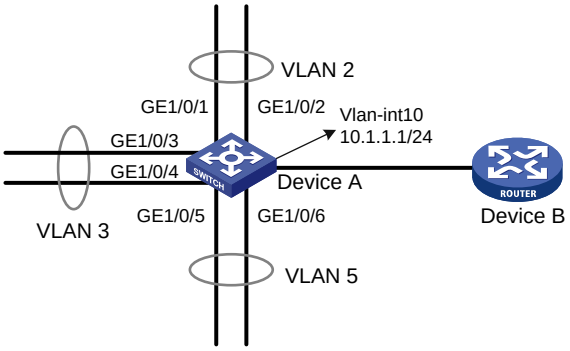
As shown in Figure 46:

- GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in VLAN 2.
- GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are in VLAN 3.
- GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 are in VLAN 5.

To save IP addresses and enable sub-VLANs to be isolated at Layer 2 but interoperable at Layer 3, perform the following tasks:

- Create a super VLAN and assign an IP address to its VLAN interface.
- Associate the super VLAN with VLANs 2, 3, and 5.

Figure 46 Network diagram



Configuration procedure

Create VLAN 10, and configure its VLAN interface IP address as 10.1.1.1/24.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
```

Enable local proxy ARP.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

Create VLAN 2, and assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the VLAN.

```
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Create VLAN 3, and assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to the VLAN.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/3 gigabitethernet 1/0/4
[DeviceA-vlan3] quit
```

Create VLAN 5, and assign GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 to the VLAN.

```
[DeviceA] vlan 5
[DeviceA-vlan5] port gigabitethernet 1/0/5 gigabitethernet 1/0/6
[DeviceA-vlan5] quit
```

Configure VLAN 10 as a super VLAN, and associate sub-VLANs 2, 3, and 5 with the super VLAN.

```
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] subvlan 2 3 5
[DeviceA-vlan10] quit
[DeviceA] quit
```

Verifying the configuration

Display information about super VLAN 10 and its associated sub-VLANs.

```
<DeviceA> display supervlan
 Super VLAN ID: 10
 Sub-VLAN ID: 2-3 5

 VLAN ID: 10
 VLAN type: Static
 It is a super VLAN.
 Route interface: Configured
 Ipv4 address: 10.1.1.1
 Ipv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged   ports: none
 Untagged ports: none

 VLAN ID: 2
 VLAN type: Static
 It is a sub VLAN.
 Route interface: Configured
 Ipv4 address: 10.1.1.1
 Ipv4 subnet mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   ports: none
 Untagged ports:
    GigabitEthernet1/0/1     GigabitEthernet1/0/2

 VLAN ID: 3
 VLAN type: Static
 It is a sub VLAN.
 Route interface: Configured
```

```
Ipv4 address: 10.1.1.1
Ipv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged   ports: none
Untagged ports:
   GigabitEthernet1/0/3     GigabitEthernet1/0/4

VLAN ID: 5
VLAN type: Static
It is a sub VLAN.
Route interface: Configured
Ipv4 address: 10.1.1.1
Ipv4 subnet mask: 255.255.255.0
Description: VLAN 0005
Name: VLAN 0005
Tagged   ports: none
Untagged ports:
   GigabitEthernet1/0/5     GigabitEthernet1/0/6
```

Configuring the private VLAN

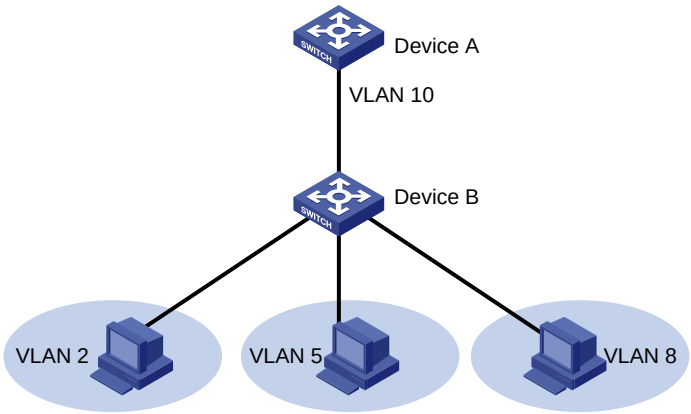
The private VLAN feature uses a two-tier VLAN structure, including a primary VLAN and secondary VLANs. This feature simplifies the network configuration and saves VLAN resources.

A primary VLAN is used for upstream data exchange. A primary VLAN can be associated with multiple secondary VLANs. Because the upstream device identifies only the primary VLAN and not the secondary VLANs, network configuration is simplified and VLAN resources are saved.

Secondary VLANs are isolated at Layer 2. To enable Layer 3 communication between secondary VLANs associated with the same primary VLAN, you can enable local proxy ARP or ND on the upstream device (for example, Device A in Figure 47).

As shown in Figure 47, the private VLAN feature is enabled on Device B. VLAN 10 is the primary VLAN. VLAN 2, VLAN 5, and VLAN 8 are secondary VLANs associated with VLAN 10 and are invisible to Device A.

Figure 47 Private VLAN example



Configuration task list

To configure the private VLAN feature, perform the following tasks:

1. Configure the primary VLAN.
2. Configure the secondary VLANs.
3. Configure the uplink and downlink ports:
   - Configure the uplink port (for example, the port connecting Device B to Device A in Figure 47):
     - When the port allows only one primary VLAN, configure the port as a promiscuous port of the primary VLAN. The promiscuous port can be automatically assigned to the primary VLAN and its associated secondary VLANs.
     - When the port allows multiple primary VLANs, configure the port as a trunk promiscuous port of the primary VLANs. The trunk promiscuous port can be automatically assigned to these primary VLANs and their associated secondary VLANs.
   - Configure a downlink port (for example, the port connecting Device B to a host in Figure 47) as a host port. The host port can be automatically assigned to the secondary VLAN and its associated primary VLAN.
   - If a downlink port allows multiple secondary VLANs, configure the port as a trunk secondary port. The trunk secondary port can be automatically assigned to the secondary VLANs and their associated primary VLANs.

For more information about promiscuous, trunk promiscuous, host, and trunk secondary ports, see *Layer 2—LAN Switching Command Reference*.

4. Associate the secondary VLANs with the primary VLAN.
5. (Optional.) Configure Layer 3 communication between the specified secondary VLANs that are associated with the primary VLAN.

Configuration restrictions and guidelines

When you configure the private VLAN feature, follow these restrictions and guidelines:

- After you complete the private VLAN configurations, perform the following tasks:
  - For a promiscuous port, make sure the following requirements are met:
    - The primary VLAN is the PVID of the port.
    - The port is an untagged member of the primary VLAN and secondary VLANs.
  - For a host port, make sure the following requirements are met:
    - The PVID of the port is a secondary VLAN.
    - The port is an untagged member of the primary VLAN and the secondary VLAN.
  - For a trunk promiscuous or trunk secondary port, make sure the port is a tagged member of the primary VLANs and the secondary VLANs.
- VLAN 1 (system default VLAN) does not support the private VLAN configuration.

Configuration procedure

To configure the private VLAN feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VLAN and enter VLAN view.	**vlan** *vlan-id*	N/A
3. Configure the VLAN as a primary VLAN.	**private-vlan primary**	By default, a VLAN is not a primary VLAN.
4. Return to system view.	**quit**	N/A
5. Create one or multiple secondary VLANs.	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	N/A
6. Enable Layer 2 communication for ports in the same secondary VLAN.	• **undo private-vlan isolated** • **private-vlan community**	Use either command. By default, ports in the same secondary VLAN can communicate with each other at Layer 2. This configuration takes effect when the following conditions exist: • The ports in the secondary VLAN are configured as host ports. • The secondary VLAN is associated with a primary VLAN.
7. Return to system view.	**quit**	N/A

Step	Command	Remarks
8. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
9. Configure the uplink port as a promiscuous or trunk promiscuous port of the specified VLANs.	• Configure the uplink port as a promiscuous port of the specified VLAN: **port private-vlan** *vlan-id* **promiscuous** • Configure the uplink port as a trunk promiscuous port of the specified VLANs: **port private-vlan** *vlan-id-list* **trunk promiscuous**	By default, a port is not a promiscuous or trunk promiscuous port of any VLAN.
10. Return to system view.	**quit**	N/A
11. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
12. Assign the downlink port to secondary VLANs.	**a.** Set the link type of the port: **port link-type** { **access** | **hybrid** | **trunk** } **b.** Assign the access port to the specified VLAN: **port access vlan** *vlan-id* **c.** Assign the trunk port to the specified VLANs: **port trunk permit vlan** { *vlan-id-list* | **all** } **d.** Assign the hybrid port to the specified VLANs: **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Select substep b, c, or d depending on the port link type.
13. Return to system view.	**quit**	N/A
14. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
15. Configure the downlink port as a host or trunk secondary port.	• Configure the downlink port as a host port: **port private-vlan host** • Configure the downlink port as a trunk secondary port: **port private-vlan** *vlan-id-list* **trunk secondary**	By default, a port is not a host or trunk secondary port.
16. Enter primary VLAN view.	**vlan** *vlan-id*	N/A
17. Associate the primary VLAN with the specified secondary VLANs.	**private-vlan secondary** *vlan-id-list*	By default, a primary VLAN is not associated with any secondary VLAN.
18. Return to system view.	**quit**	N/A

Step	Command	Remarks
19. (Optional.) Configure Layer 3 communication between the specified secondary VLANs.	**a.** Enter VLAN interface view of the primary VLAN interface: **interface vlan-interface** *vlan-id* **b.** Enable Layer 3 communication between secondary VLANs that are associated with the primary VLAN: **private-vlan secondary** *vlan-id-list* **c.** Assign an IPv4 address to the primary VLAN interface: **ip address** *ip-address* { *mask-length* | *mask* } [**sub**] **d.** Assign an IPv6 address to the primary VLAN interface: **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **e.** Enable local proxy ARP: **local-proxy-arp enable** **f.** Enable local proxy ND: **local-proxy-nd enable**	Use substeps a, b, c, and e for devices that run IPv4 protocols. Use substeps a, b, d, and f for devices that run IPv6 protocols. By default: • Secondary VLANs cannot communicate with each other at Layer 3. • No IP address is configured for a VLAN interface. • Local proxy ARP and local proxy ND are disabled.

Displaying and maintaining the private VLAN

Execute **display** commands in any view.

Task	Command
Display information about primary VLANs and the secondary VLANs associated with each primary VLAN.	**display private-vlan** [*primary-vlan-id*]

Private VLAN configuration examples

Promiscuous port configuration example

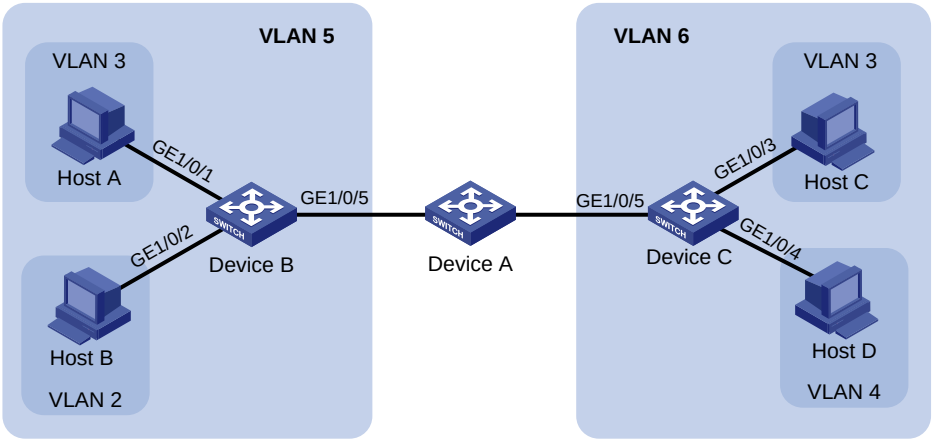
Network requirements

As shown in Figure 48, configure the private VLAN feature to meet the following requirements:

- On Device B, VLAN 5 is a primary VLAN that is associated with secondary VLANs 2 and 3. GigabitEthernet 1/0/5 is in VLAN 5. GigabitEthernet 1/0/2 is in VLAN 2. GigabitEthernet 1/0/1 is in VLAN 3.

- On Device C, VLAN 6 is a primary VLAN that is associated with secondary VLANs 3 and 4. GigabitEthernet 1/0/5 is in VLAN 6. GigabitEthernet 1/0/3 is in VLAN 3. GigabitEthernet 1/0/4 is in VLAN 4.
- Device A is aware of only VLAN 5 on Device B and VLAN 6 on Device C.

Figure 48 Network diagram



Configuration procedure

This example describes the configurations on Device B and Device C.

1. Configure Device B:

Configure VLAN 5 as a primary VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
```

Create VLANs 2 and 3.

```
[DeviceB] vlan 2 to 3
```

Configure the uplink port GigabitEthernet 1/0/5 as a promiscuous port of VLAN 5.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port private-vlan 5 promiscuous
[DeviceB-GigabitEthernet1/0/5] quit
```

Assign the downlink port GigabitEthernet 1/0/1 to VLAN 3, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 3
[DeviceB-GigabitEthernet1/0/1] port private-vlan host
[DeviceB-GigabitEthernet1/0/1] quit
```

Assign the downlink port GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

Associate the secondary VLANs 2 and 3 with the primary VLAN 5.

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
```

```
[DeviceB-vlan5] quit
```

2. Configure Device C:

   # Configure VLAN 6 as a primary VLAN.

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC–vlan6] private-vlan primary
[DeviceC–vlan6] quit
```

   # Create VLANs 3 and 4.

```
[DeviceC] vlan 3 to 4
```

   # Configure the uplink port GigabitEthernet 1/0/5 as a promiscuous port of VLAN 6.

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port private-vlan 6 promiscuous
[DeviceC-GigabitEthernet1/0/5] quit
```

   # Assign the downlink port GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 3
[DeviceC-GigabitEthernet1/0/3] port private-vlan host
[DeviceC-GigabitEthernet1/0/3] quit
```

   # Assign the downlink port GigabitEthernet 1/0/4 to VLAN 4, and configure the port as a host port.

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] port access vlan 4
[DeviceC-GigabitEthernet1/0/4] port private-vlan host
[DeviceC-GigabitEthernet1/0/4] quit
```

   # Associate the secondary VLANs 3 and 4 with the primary VLAN 6.

```
[DeviceC] vlan 6
[DeviceC-vlan6] private-vlan secondary 3 to 4
[DeviceC-vlan6] quit
```

Verifying the configuration

Display the private VLAN configuration on the devices, for example, on Device B.

```
[DeviceB] display private-vlan
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged   ports: None
 Untagged ports:
    GigabitEthernet1/0/1           GigabitEthernet1/0/2           GigabitEthernet1/0/5

 VLAN ID: 2
 VLAN type: Static
```

```
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged   ports: None
Untagged ports:
   GigabitEthernet1/0/2            GigabitEthernet1/0/5

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: None
Untagged Ports:
   GigabitEthernet1/0/1            GigabitEthernet1/0/5
```

The output shows that:

- The promiscuous port GigabitEthernet 1/0/5 is an untagged member of primary VLAN 5 and secondary VLANs 2 and 3.
- The host port GigabitEthernet 1/0/2 is an untagged member of primary VLAN 5 and secondary VLAN 2.
- The host port GigabitEthernet 1/0/1 is an untagged member of primary VLAN 5 and secondary VLAN 3.

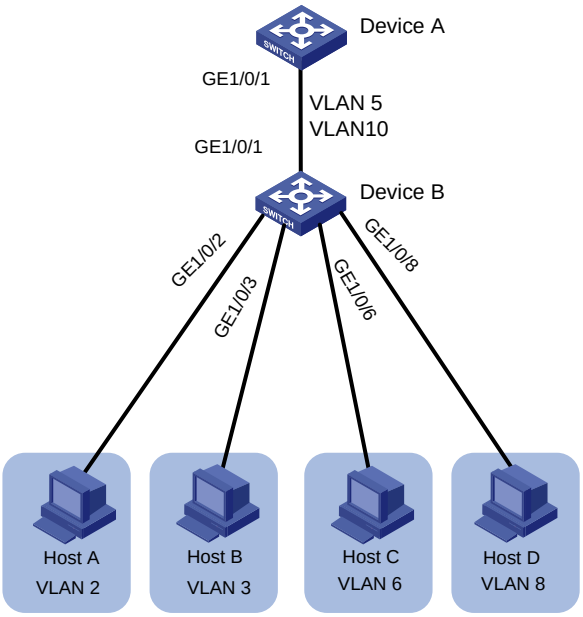
Trunk promiscuous port configuration example

Network requirements

As shown in Figure 49, configure the private VLAN feature to meet the following requirements:

- VLANs 5 and 10 are primary VLANs on Device B. The uplink port GigabitEthernet 1/0/1 on Device B permits the packets from VLANs 5 and 10 to pass through tagged.
- On Device B, the downlink port GigabitEthernet 1/0/2 permits secondary VLAN 2. The downlink port GigabitEthernet 1/0/3 permits secondary VLAN 3. Secondary VLANs 2 and 3 are associated with primary VLAN 5.
- On Device B, the downlink port GigabitEthernet 1/0/6 permits secondary VLAN 6. The downlink port GigabitEthernet 1/0/8 permits secondary VLAN 8. Secondary VLANs 6 and 8 are associated with primary VLAN 10.
- Device A is aware of only VLANs 5 and 10 on Device B.

Figure 49 Network diagram



Configuration procedure

1. Configure Device B:

   # Configure VLANs 5 and 10 as primary VLANs.

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

   # Create VLANs 2, 3, 6, and 8.

```
[DeviceB] vlan 2 to 3
[DeviceB] vlan 6
[DeviceB-vlan6] quit
[DeviceB] vlan 8
[DeviceB-vlan8] quit
```

   # Configure the uplink port GigabitEthernet 1/0/1 as a trunk promiscuous port of VLANs 5 and 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 5 10 trunk promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

   # Assign the downlink port GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

   # Assign the downlink port GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

Associate the secondary VLANs 2 and 3 with the primary VLAN 5.

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

Assign the downlink port GigabitEthernet 1/0/6 to VLAN 6, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port access vlan 6
[DeviceB-GigabitEthernet1/0/6] port private-vlan host
[DeviceB-GigabitEthernet1/0/6] quit
```

Assign the downlink port GigabitEthernet 1/0/8 to VLAN 8, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/8
[DeviceB-GigabitEthernet1/0/8] port access vlan 8
[DeviceB-GigabitEthernet1/0/8] port private-vlan host
[DeviceB-GigabitEthernet1/0/8] quit
```

Associate the secondary VLANs 6 and 8 with the primary VLAN 10.

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 6 8
[DeviceB-vlan10] quit
```

2. Configure Device A:

Create VLANs 5 and 10.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 5 and 10 as a tagged VLAN member.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display primary VLAN configurations on Device B. The following output uses primary VLAN 5 as an example.

```
[DeviceB] display private-vlan 5
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
```

```
Name: VLAN 0005
Tagged   ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/2          GigabitEthernet1/0/3

VLAN ID: 2
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged   ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/2

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged   ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/3
```

The output shows that:

- The trunk promiscuous port GigabitEthernet 1/0/1 is a tagged member of primary VLAN 5 and secondary VLANs 2 and 3.
- The host port GigabitEthernet 1/0/2 is an untagged member of primary VLAN 5 and secondary VLAN 2.
- The host port GigabitEthernet 1/0/3 is an untagged member of primary VLAN 5 and secondary VLAN 3.

Trunk promiscuous and trunk secondary port configuration example

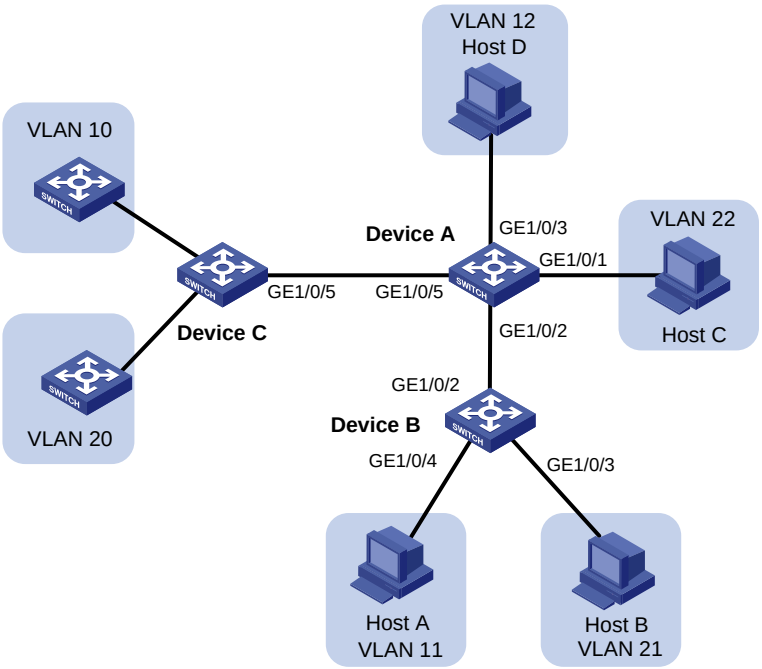
Network requirements

As shown in Figure 50, configure the private VLAN feature to meet the following requirements:

- VLANs 10 and 20 are primary VLANs on Device A. The uplink port GigabitEthernet 1/0/5 on Device A permits the packets from VLANs 10 and 20 to pass through tagged.
- VLAN 11, VLAN 12, VLAN 21, and VLAN 22 are secondary VLANs on Device A.
  - The downlink port GigabitEthernet 1/0/2 permits the packets from VLAN 11 and VLAN 21 to pass through tagged.
  - The downlink port GigabitEthernet 1/0/1 permits VLAN 22.
  - The downlink port GigabitEthernet 1/0/3 permits VLAN 12.

- Secondary VLANs 11 and 12 are associated with primary VLAN 10.
- Secondary VLANs 21 and 22 are associated with primary VLAN 20.

Figure 50 Network diagram



Configuration procedure

1. Configure Device A:

   # Configure VLANs 10 and 20 as primary VLANs.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan primary
[DeviceA-vlan20] quit
```

   # Create VLANs 11, 12, 21, and 22, which are to be configured as secondary VLANs.

```
[DeviceA] vlan 11 to 12
[DeviceA] vlan 21 to 22
```

   # Associate the secondary VLANs 11 and 12 with the primary VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 11 12
[DeviceA-vlan10] quit
```

   # Associate the secondary VLANs 21 and 22 with the primary VLAN 20.

```
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan secondary 21 22
[DeviceA-vlan20] quit
```

   # Configure the uplink port GigabitEthernet 1/0/5 as a trunk promiscuous port of VLANs 10 and 20.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port private-vlan 10 20 trunk promiscuous
```

```
[DeviceA-GigabitEthernet1/0/5] quit
```

Assign the downlink port GigabitEthernet 1/0/1 to VLAN 22 and configure the port as a host port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 22
[DeviceA-GigabitEthernet1/0/1] port private-vlan host
[DeviceA-GigabitEthernet1/0/1] quit
```

Assign the downlink port GigabitEthernet 1/0/3 to VLAN 12 and configure the port as a host port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 12
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

Configure the downlink port GigabitEthernet 1/0/2 as a trunk secondary port in VLANs 11 and 21.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port private-vlan 11 21 trunk secondary
[DeviceA-GigabitEthernet1/0/2] quit
```

2. Configure Device B:

Create VLANs 11 and 21.

```
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit
```

Configure GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLANs 11 and 21 as a tagged VLAN member.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type hybrid
[DeviceB-GigabitEthernet1/0/2] port hybrid vlan 11 21 tagged
[DeviceB-GigabitEthernet1/0/2] quit
```

Assign the port GigabitEthernet 1/0/4 to VLAN 11.

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 11
[DeviceB-GigabitEthernet1/0/4] quit
```

Assign the port GigabitEthernet 1/0/3 to VLAN 21.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 21
[DeviceB-GigabitEthernet1/0/3] quit
```

3. Configure Device C:

Create VLANs 10 and 20.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
```

Configure GigabitEthernet1/0/5 as a hybrid port, and assign it to VLANs 10 and 20 as a tagged VLAN member.

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port link-type hybrid
[DeviceC-GigabitEthernet1/0/5] port hybrid vlan 10 20 tagged
[DeviceC-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Display the configuration of primary VLAN 10 on Device A.

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 11-12

 VLAN ID: 10
 VLAN type: Static
 Private-vlan type: Primary
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged   ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/3

 VLAN ID: 11
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0011
 Name: VLAN 0011
 Tagged   ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/5
 Untagged ports: None

VLAN ID: 12
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0012
 Name: VLAN 0012
 Tagged   ports:
    GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/3
```

The output shows that:

- The trunk promiscuous port GigabitEthernet 1/0/5 is a tagged member of primary VLAN 10 and secondary VLANs 11 and 12.
- The trunk secondary port GigabitEthernet 1/0/2 is a tagged member of primary VLAN 10 and secondary VLAN 11.
- The host port GigabitEthernet 1/0/3 is an untagged member of primary VLAN 10 and secondary VLAN 12.

Display the configuration of primary VLAN 20 on Device A.

```
[DeviceA] display private-vlan 20
 Primary VLAN ID: 20
 Secondary VLAN ID: 21-22

 VLAN ID: 20
 VLAN type: Static
 Private-vlan type: Primary
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged   ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/1

 VLAN ID: 21
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0021
 Name: VLAN 0021
 Tagged   ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/5
 Untagged ports: None

 VLAN ID: 22
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0022
 Name: VLAN 0022
 Tagged   ports:
    GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/1
```

The output shows that:

- The trunk promiscuous port GigabitEthernet 1/0/5 is a tagged member of primary VLAN 20 and secondary VLANs 21 and 22.
- The trunk secondary port GigabitEthernet 1/0/2 is a tagged member of primary VLAN 20 and secondary VLAN 21.
- The host port GigabitEthernet 1/0/1 is an untagged member of primary VLAN 20 and secondary VLAN 22.

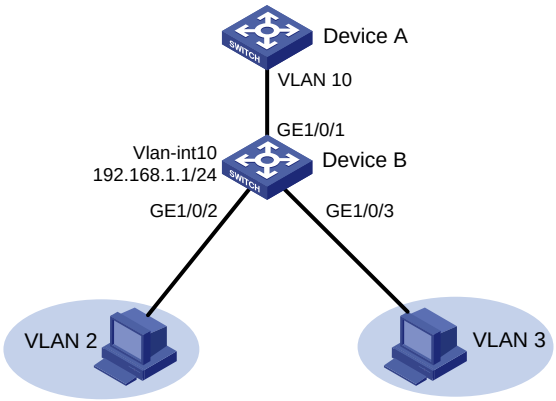
Secondary VLAN Layer 3 communication configuration example

Network requirements

As shown in Figure 51, configure the private VLAN feature to meet the following requirements:

- Primary VLAN 10 on Device B is associated with secondary VLANs 2 and 3.
- The uplink port GigabitEthernet 1/0/1 is in VLAN 10.
- The IP address of VLAN-interface 10 is 192.168.1.1/24.
- The ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are in VLAN 2 and VLAN 3, respectively.
- Secondary VLANs are isolated at Layer 2 but interoperable at Layer 3.

Figure 51 Network diagram



Configuration procedure

Create VLAN 2 and VLAN 3.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 3
```

Configure VLAN 10 as a primary VLAN, and associate VLAN 2 and VLAN 3 with primary VLAN 10 as secondary VLANs.

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] private-vlan secondary 2 3
[DeviceB-vlan10] quit
```

Configure the uplink port GigabitEthernet 1/0/1 as a promiscuous port of VLAN 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

Assign the downlink port GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

Assign the downlink port GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceB] interface gigabitethernet 1/0/3
```

```
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

Enable Layer 3 communication between secondary VLANs 2 and 3 that are associated with primary VLAN 10.

```
[DeviceB] interface vlan-interface 10
[DeviceB-Vlan-interface10] private-vlan secondary 2 3
```

Assign the IP address 192.168.1.1/24 to VLAN-interface 10.

```
[DeviceB-Vlan-interface10] ip address 192.168.1.1 255.255.255.0
```

Enable local proxy ARP on VLAN-interface 10.

```
[DeviceB-Vlan-interface10] local-proxy-arp enable
[DeviceB-Vlan-interface10] quit
```

Verifying the configuration

Display the configuration of primary VLAN 10.

```
[DeviceB] display private-vlan 10
 Primary VLAN ID: 10
 Secondary-VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged   ports: None
 Untagged ports:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   ports: None
 Untagged ports:
    GigabitEthernet1/0/1            GigabitEthernet1/0/2

 VLAN ID: 3
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
```

```
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged   ports: None
Untagged ports:
   GigabitEthernet1/0/1            GigabitEthernet1/0/3
```

The **Route interface** field in the output is **Configured**, indicating that secondary VLANs 2 and 3 are interoperable at Layer 3.

Configuring voice VLANs

Overview

A voice VLAN is used for transmitting voice traffic. When ports that connect to voice devices are assigned to a voice VLAN, the system can configure QoS parameters for voice packets to ensure higher transmission priority and sound voice quality.

Common voice devices include IP phones and integrated access devices (IADs). This chapter uses IP phone as an example.

For an IP phone to access a device, the device must perform the following operations:

- Identify the IP phone in the network and obtain the MAC address of the IP phone.
- Advertise the voice VLAN information to the IP phone.

After receiving the voice VLAN information, the IP phone can perform automatic configuration, so the voice packets sent from the IP phone can be transmitted within the voice VLAN.

Methods of identifying IP phones

Devices can use the OUI addresses or LLDP to identify IP phones.

Identifying IP phones through OUI addresses

A device determines whether a received packet is a voice packet based on its source MAC address. A packet whose source MAC address complies with any of the Organizationally Unique Identifier (OUI) addresses of the voice devices is regarded as voice traffic.

You can use system default OUI addresses (see Table 11) or configure OUI addresses for the device. You can manually remove or add the system default OUI addresses.

The switch supports 128 OUI addresses, including system default OUI addresses.

Table 11 Default OUI addresses

Number	OUI address	Vendor
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	00D0-1E00-0000	Pingtel phone
5	0060-B900-0000	Philips/NEC phone
6	00E0-7500-0000	Polycom phone
7	00E0-BB00-0000	3Com phone

Typically, an OUI address refers to the first 24 bits of a MAC address (in binary notation) and is a globally unique identifier that IEEE assigns to a vendor. However, OUI addresses in this chapter are addresses that the system uses to determine whether a received packet is a voice packet. They are the logical AND results of the *mac-address* and *oui-mask* arguments in the **voice-vlan mac-address** command.

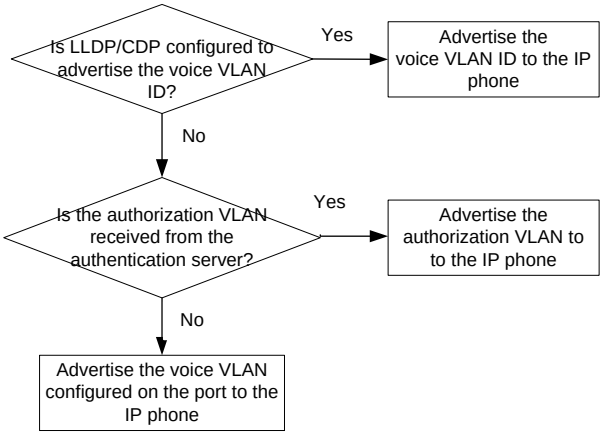
Automatically identifying IP phones through LLDP

When you use OUI addresses to identify IP phones, the number of OUI addresses that can be configured is limited. Additionally, when there are plenty of IP phones in the network, you must configure many OUI addresses. If IP phones support LLDP, configure LLDP on the device for automatic IP phone discovery. For more information, see "Enabling LLDP for automatic IP phone discovery."

Advertising the voice VLAN information to IP phones

Figure 52 shows the workflow of advertising the voice VLAN information to IP phones.

Figure 52 Workflow of advertising the voice VLAN information to IP phones



After receiving the voice VLAN information, the IP phone automatically completes the voice VLAN configuration.

- If the voice VLAN configuration is based on the received LLDP-MED TLVs or CDP packets, the IP phone will send out packets tagged with the advertised voice VLAN ID. The voice packets will be forwarded in the voice VLAN.

  For more information about configuring LLDP or CDP, see "Configuring LLDP or CDP to advertise a voice VLAN." For more information about LLDP and CDP compatibility, see "Configuring LLDP."

- If the voice VLAN configuration is based on the authorization VLAN information, the IP phone will send out packets tagged with the advertised authorization VLAN ID. The voice packets will be forwarded in the authorization VLAN.

  For more information about advertising the authorization VLAN information to IP phones, see "Dynamically advertising an authorization VLAN through LLDP or CDP." For more information about authorization VLANs, see *Security Configuration Guide*.

- If the voice VLAN configuration is based on the voice VLAN information of the accessing port, the voice traffic from the IP phone will be forwarded in the voice VLAN of the accessing port. Whether the voice packets are tagged depends on the voice VLAN configuration of the accessing port. For more information about configuring a voice VLAN on a port, see "Configuring a voice VLAN on a port."

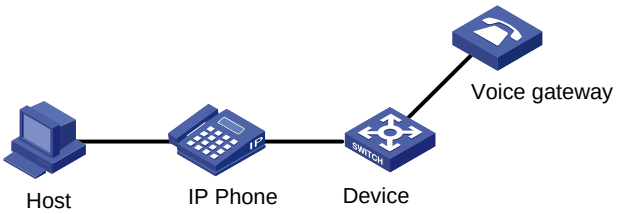
IP phone access methods

Connecting the host and the IP phone in series

As shown in Figure 53, the host is connected to the IP phone, and the IP phone is connected to the device. In this scenario, the following requirements must be met:

- The host and the IP phone use different VLANs.
- The IP phone is able to send out VLAN-tagged packets, so that the device can differentiate traffic from the host and the IP phone.
- The port connecting to the IP phone forwards packets from the voice VLAN and the PVID.

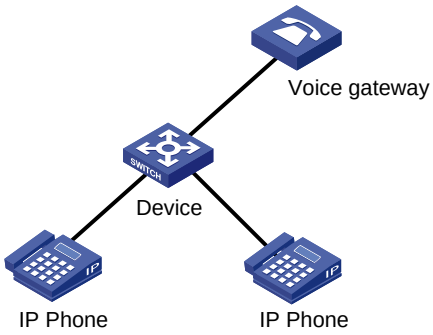
Figure 53 Connecting the host and IP phone in series



Connecting the IP phone to the device

As shown in Figure 54, the IP phone is connected to the device without the presence of the host. Use this connection method when the IP phone sends out untagged voice packets. In this scenario, you must configure the voice VLAN as the PVID of the port, and configure the port to forward the packets from the PVID.

Figure 54 Connecting the IP phone to the device



Configuring a voice VLAN on a port

Voice VLAN assignment modes

A port can be assigned to a voice VLAN automatically or manually.

Automatic mode

Use automatic mode when PCs and IP phones are connected in series to access the network through the device, as shown in Figure 53. Ports on the device transmit both voice traffic and data traffic.

When an IP phone is powered on, it sends out protocol packets. After receiving these protocol packets, the device uses the source MAC address of the protocol packets to match its OUI addresses. If the match succeeds, the system performs the following operations:

- Assigns the receiving port of the protocol packets to the voice VLAN.
- Issues ACL rules to set the packet precedence.
- Starts the voice VLAN aging timer.

The system will remove the port from the voice VLAN if no packet is received from the port before the aging timer expires. The aging timer is also configurable.

If the device reboots, the port is reassigned to the voice VLAN to ensure the correct operation of the existing voice connections. The reassignment occurs automatically without being triggered by voice traffic as long as the voice VLAN operates correctly.

Manual mode

Use manual mode when only IP phones access the network through the device, as shown in Figure 54. In this mode, ports are assigned to a voice VLAN that transmits voice traffic exclusively. No data traffic affects the voice traffic transmission.

You must manually assign the receiving port on the device to a voice VLAN. The device uses the source MAC address of the received voice packets to match its OUI addresses. If the match succeeds, the system issues ACL rules to set the packet precedence.

To remove the port from the voice VLAN, you must manually remove it.

Cooperation of voice VLAN assignment modes and IP phones

Some IP phones send out VLAN-tagged packets, and others send out only untagged packets. For correct packet processing, ports of different link types must meet specific configuration requirements in different voice VLAN assignment modes.

Table 12 Configuration requirements for access/trunk/hybrid ports to support tagged voice traffic

Port link type	Voice VLAN assignment mode	Support for tagged voice traffic	Configuration requirements
Access	Automatic	No	N/A
	Manual	No	N/A
Trunk	Automatic	Yes	The PVID of the port cannot be the voice VLAN.
	Manual	Yes	The PVID of the port cannot be the voice VLAN. Configure the port to forward the packets from the voice VLAN.
Hybrid	Automatic	Yes	The PVID of the port cannot be the voice VLAN.
	Manual	Yes	The PVID of the port cannot be the voice VLAN. Configure the port to forward the packets from the voice VLAN with VLAN tags.

Table 13 Configuration requirements for access/trunk/hybrid ports to support untagged voice traffic

Port link type	Voice VLAN assignment mode	Support for untagged voice traffic	Configuration requirements
Access	Automatic	No	N/A
	Manual	Yes	Configure the voice VLAN as the PVID of the port.
Trunk	Automatic	No	N/A
	Manual	Yes	Configure the voice VLAN as the PVID of the port. Configure the port to forward the packets from the voice VLAN.
Hybrid	Automatic	No	N/A
	Manual	Yes	Configure the voice VLAN as the PVID of the port. Configure the port to forward the packets from the voice VLAN without VLAN tags.

If an IP phone sends out tagged voice traffic, and its accessing port is configured with 802.1X authentication, guest VLAN, Auth-Fail VLAN, or critical VLAN, the VLAN ID must be different for the following VLANs:

- Voice VLAN.
- PVID of the accessing port.
- 802.1X guest, Auth-Fail, or critical VLAN.

If an IP phone sends out untagged voice traffic, the PVID of the accessing port must be the voice VLAN. As a result, 802.1X authentication is not supported.

Security mode and normal mode of voice VLANs

Depending on the incoming packet filtering mechanisms, a voice VLAN-enabled port can operate in one of the following modes:

- **Normal mode**—The port receives voice-VLAN-tagged packets and forwards them in the voice VLAN without examining their MAC addresses. If the PVID of the port is the voice VLAN and the port operates in manual VLAN assignment mode, the port forwards all the received untagged packets in the voice VLAN.

  In this mode, voice VLANs are vulnerable to traffic attacks. Malicious users might send large quantities of forged voice-VLAN-tagged or untagged packets to consume the voice VLAN bandwidth to affect normal voice communication.
- **Security mode**—The port uses the source MAC addresses of voice packets to match the OUI addresses of the device. Packets that fail the match will be dropped.

In a safe network, you can configure the voice VLANs to operate in normal mode to reduce the system resource consumption in source MAC address checking.

TIP:

As a best practice, do not transmit both voice traffic and non-voice traffic in a voice VLAN. If you must transmit different traffic in a voice VLAN, make sure the voice VLAN security mode is disabled.

Table 14 Packet processing on a voice VLAN-enabled port in normal and security mode

Voice VLAN mode	Packet type	Packet processing
Normal	Untagged packets or packets with the voice VLAN tags	The port does not examine the source MAC addresses of incoming packets. Both voice traffic and non-voice traffic can be transmitted in the voice VLAN.
	Packets with other VLAN tags	Forwarded or dropped depending on whether the port allows packets from these VLANs to pass through.
Security	Untagged packets or packets with the voice VLAN tags	• If the source MAC address of a packet matches an OUI address on the device, the packet is forwarded in the voice VLAN. • If the source MAC address of a packet does not match an OUI address on the device, the packet is dropped.
	Packets with other VLAN tags	Forwarded or dropped depending on whether the port allows packets from these VLANs to pass through.

Configuration prerequisites

Before you configure a voice VLAN, complete the following tasks:

- Create a VLAN.
- Determine the QoS priority settings for voice VLAN traffic.
- Determine the voice VLAN assignment mode.

Configuring the QoS priority settings for voice traffic

The QoS priority settings carried in voice traffic include the CoS and DSCP values. You can configure the device to modify the QoS priority settings for voice traffic.

Before you configure the QoS priority settings for voice traffic on a port, make sure the voice VLAN feature is disabled on it.

To configure the QoS priority settings for voice traffic:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure QoS priority settings for incoming voice VLAN packets.	• Configure the port to trust and retain the QoS priority settings: **a.** Use the 802.1p priority in incoming packets for priority mapping: **qos trust dot1p** **b.** Configure the port to trust and retain the QoS priority settings: **voice-vlan qos trust** • Configure the port to modify the CoS and DSCP values: **voice-vlan qos** *cos-value dscp-value*	By default, a port modifies the CoS and DSCP values for voice VLAN packets to 6 and 46, respectively. If you execute the **voice-vlan qos** and **voice-vlan qos trust** commands multiple times, the most recent configuration takes effect. For more information about the **qos trust dot1p** command, see *ACL and QoS Command Reference*.

Configuring a port to operate in automatic voice VLAN assignment mode

Configuration restrictions and guidelines

When you configure a port to operate in automatic voice VLAN assignment mode, follow these restrictions and guidelines:

- Do not configure a VLAN as both a voice VLAN and a protocol-based VLAN. A voice VLAN in automatic mode on a hybrid port processes only tagged incoming voice traffic. A protocol-based VLAN on a hybrid port processes only untagged incoming packets. For more information about protocol-based VLANs, see "Configuring protocol-based VLANs."
- As a best practice, do not use the automatic voice VLAN assignment mode together with MSTP. In MSTP mode, if a port is blocked in the MSTI of the target voice VLAN, the port drops the received packets instead of delivering them to the CPU. As a result, the receiving port will not be dynamically assigned to the voice VLAN.
- As a best practice, do not use the automatic voice VLAN assignment mode together with PVST. In PVST mode, if the target voice VLAN is not permitted on a port, the port is placed in blocked state. The received packets are dropped instead of being delivered to the CPU. As a result, the receiving port will not be dynamically assigned to the voice VLAN.
- As a best practice, do not configure both dynamic MAC-based VLAN assignment and automatic voice VLAN assignment mode on a port. If you have to configure both of them on a port, configure dynamic MAC-based VLAN assignment first. If you configure them in a reverse order, conflict will occur. When you remove one of the configurations, the operation of the other is affected.

Configuration procedure

To configure a port to operate in automatic voice VLAN assignment mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Set the voice VLAN aging timer.	**voice-vlan aging** *minutes*	By default, the aging timer of a voice VLAN is 1440 minutes. The voice VLAN aging timer takes effect only on ports in automatic voice VLAN assignment mode.
3. (Optional.) Enable the voice VLAN security mode.	**voice-vlan security enable**	By default, the voice VLAN security mode is enabled.
4. (Optional.) Add an OUI address for voice packet identification.	**voice-vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	By default, system default OUI addresses exist. For more information, see Table 11.
5. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
6. Configure the link type of the port.	• **port link-type trunk** • **port link-type hybrid**	N/A
7. (Optional.) Configure the port to operate in automatic voice VLAN assignment mode.	**voice-vlan mode auto**	By default, the automatic voice VLAN assignment mode is enabled.
8. Enable the voice VLAN feature on the port.	**voice-vlan** *vlan-id* **enable**	By default, the voice VLAN feature is disabled.

Configuring a port to operate in manual voice VLAN assignment mode

Configuration restrictions and guidelines

When you configure a port to operate in manual voice VLAN assignment mode, follow these restrictions and guidelines:

- You can configure different voice VLANs on different ports on the same device. Make sure the following requirements are met:
  - One port can be configured with only one voice VLAN.
  - Voice VLANs must be existing static VLANs.
- Do not enable voice VLAN on the member ports of a link aggregation group. For more information about link aggregation, see "Configuring Ethernet link aggregation."
- For a port that is enabled with voice VLAN and operating in manual mode, you must manually assign the port to the voice VLAN to make the voice VLAN take effect.

Configuration procedure

To configure a port to operate in manual voice VLAN assignment mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Enable the voice VLAN security mode.	**voice-vlan security enable**	By default, the voice VLAN security mode is enabled.
3. (Optional.) Add an OUI address for voice packet identification.	**voice-vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	By default, system default OUI addresses exist. For more information, see Table 11.
4. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
5. Configure the port to operate in manual voice VLAN assignment mode.	**undo voice-vlan mode auto**	By default, the manual voice VLAN assignment mode is disabled.
6. Assign the access, trunk, or hybrid port in manual voice VLAN assignment mode to the voice VLAN.	• For the access port, see "Assigning an access port to a VLAN." • For the trunk port, see "Assigning a trunk port to a VLAN." • For the hybrid port, see "Assigning a hybrid port to a VLAN."	After you assign an access port to the voice VLAN, the voice VLAN becomes the PVID of the port.
7. (Optional.) Configure the voice VLAN as the PVID of the trunk or hybrid port.	• For the trunk port, see "Assigning a trunk port to a VLAN." • For the hybrid port, see "Assigning a hybrid port to a VLAN."	This step is required for untagged incoming voice traffic and prohibited for tagged incoming voice traffic.
8. Enable the voice VLAN feature on the port.	**voice-vlan** *vlan-id* **enable**	By default, the voice VLAN feature is disabled.

Enabling LLDP for automatic IP phone discovery

The device can automatically discover the peer through LLDP, and exchange LLDP TLVs with the peer. If the LLDP System Capabilities TLV received on a port indicates that the peer can act as a telephone, the device sends an LLDP TLV with the voice VLAN configuration to the peer.

When the IP phone discovery process is complete, the port will continue the following voice VLAN configuration:

- Join the voice VLAN.
- Increase the transmission priority of the voice traffic sent from the IP phone.

To ensure that the IP phone can pass authentication, the device will add the MAC address of the IP phone to the MAC address table.

Configuration prerequisites

Before you enable LLDP for automatic IP phone discovery, complete the following tasks:

- Enable LLDP globally and on ports.
- Complete voice VLAN configurations.

Configuration restrictions and guidelines

When you enable LLDP for automatic IP phone discovery, following these restrictions and guidelines:

- A maximum of five IP phones can be connected to each port of the device.
- Use this feature only with the automatic voice VLAN assignment mode.
- You cannot use this feature together with CDP compatibility.

Configuration procedure

To enable LLDP for automatic IP phone discovery:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable LLDP for automatic IP phone discovery.	**voice-vlan track lldp**	By default, this function is disabled.

Configuring LLDP or CDP to advertise a voice VLAN

If IP phones support LLDP, the device advertises the voice VLAN information to the IP phones through the LLDP-MED TLVs. If IP phones support only CDP, configure CDP compatibility on the device to enable it to advertise the voice VLAN information through CDP packets.

In either case, the voice VLAN information includes the voice VLAN ID and the tagging status indicator of the voice packets. The LLDP packets sent from the device carry the priority information. The CDP packets sent from the device do not carry the priority information.

By default, if a voice VLAN is configured on the port connected to the IP phone, the device advertises this voice VLAN to the IP phone. The device learns the MAC address of the IP phone and increases the priority for voice packets. The address learning is implemented in software.

In an IRF fabric, MAC address learning and synchronization of the learned MAC address entry to all member devices in software results in an undesirable delay. In this case, you can use this feature to configure LLDP or CDP to advertise the voice VLAN ID. Then, the IRF fabric learns and synchronizes MAC address entries faster in hardware.

After you configure this feature, the device advertises the voice VLAN to the IP phone by following the workflow described in Figure 52.

To configure LLDP or CDP to advertise a voice VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure LLDP or CDP to advertise a voice VLAN.	• Configure LLDP to advertise a voice VLAN: **lldp tlv-enable med-tlv network-policy** *vlan-id* • Configure CDP to advertise a voice VLAN: **a.** Specify the ID of an advertised VLAN: **cdp voice-vlan** *vlan-id* **b.** Configure CDP compatibility: For more information, see "Configuring LLDP."	By default, LLDP and CDP advertise the voice VLAN configured on the port. For more information about the **lldp tlv-enable med-tlv network-policy** command, see *Layer 2—LAN Switching Command Reference*.
4. (Optional.) Display the voice VLAN advertised by LLDP.	**display lldp local-information**	The advertised voice LAN information is displayed in the **MED information** fields in the command output.

Dynamically advertising an authorization VLAN through LLDP or CDP

This function is available only on IP phones that support LLDP or CDP.

Dynamic authorization VLAN advertisement through LLDP or CDP works with 802.1X or MAC authentication. If 802.1X authentication is used, make sure the IP phone support 802.1X authentication.

After the IP phone passes authentication, LLDP advertises the authorization VLAN in the LLDP-MED Network Policy TLV to the IP phone. If the IP phone supports only CDP, CDP advertises the authorization VLAN in CDP packets to the IP phone. The port connected to the IP phone will be added to the authorization VLAN.

To implement this function, perform the following configuration tasks:

1. Enable LLDP globally and on the port connected to the IP phone.

   If the IP phone supports only CDP, configure CDP compatibility on the device.
2. Configure 802.1X or MAC authentication to ensure that the IP phone can pass security authentication. For more information about 802.1X and MAC authentication, see *Security Configuration Guide*.

3. Configure the authorization VLAN for the IP phone on the authentication server. For more information about authorization VLANs, see *Security Configuration Guide*.

Displaying and maintaining voice VLANs

Execute **display** commands in any view.

Task	Command
Display the voice VLAN state.	**display voice-vlan state**
Display the OUI addresses that the system supports.	**display voice-vlan mac-address**

Voice VLAN configuration examples

Automatic voice VLAN assignment mode configuration example

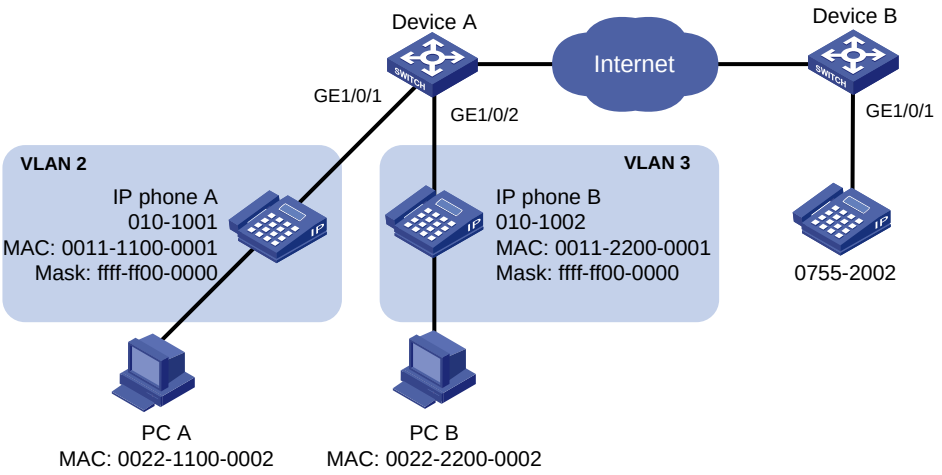
Network requirements

As shown in Figure 55, Device A transmits traffic from IP phones and hosts.

For correct voice traffic transmission, perform the following tasks on Device A:

- Configure voice VLANs 2 and 3 to transmit voice packets from IP phones A and B, respectively.
- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to operate in automatic voice VLAN assignment mode.
- Add MAC addresses of IP phones A and B to the device for voice packet identification. The mask of the two MAC addresses is FFFF-FF00-0000.

Figure 55 Network diagram



Configuration procedure

1. Configure voice VLANs:

   # Create VLANs 2 and 3.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 2 to 3
   ```

Set the voice VLAN aging timer to 30 minutes.

```
[DeviceA] voice-vlan aging 30
```

Configure voice VLANs to operate in security mode to transmit only voice packets.

```
[DeviceA] voice-vlan security enable
```

Add MAC addresses of IP phones A and B to the device with the mask FFFF-FF00-0000.

```
[DeviceA] voice-vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP
phone A
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP
phone B
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

Configure GigabitEthernet 1/0/1 to operate in automatic voice VLAN assignment mode.

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan mode auto
```

Enable voice VLAN on GigabitEthernet 1/0/1 and configure VLAN 2 as the voice VLAN for it.

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a hybrid port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
```

Configure GigabitEthernet 1/0/2 to operate in automatic voice VLAN assignment mode.

```
[DeviceA-GigabitEthernet1/0/2] voice-vlan mode auto
```

Enable voice VLAN on GigabitEthernet 1/0/2 and configure VLAN 3 as the voice VLAN for it.

```
[DeviceA-GigabitEthernet1/0/2] voice-vlan 3 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display the OUI addresses and their masks and descriptions.

```
[DeviceA] display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the voice VLAN state.

```
[DeviceA] display voice-vlan state
 Current Voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled ports and their modes:
 Port                            VLAN        Mode        COS        DSCP
 GigabitEthernet1/0/1            2           AUTO        6          46
```

```
GigabitEthernet1/0/2            3            AUTO        6           46
```

Manual voice VLAN assignment mode configuration example

Network requirements

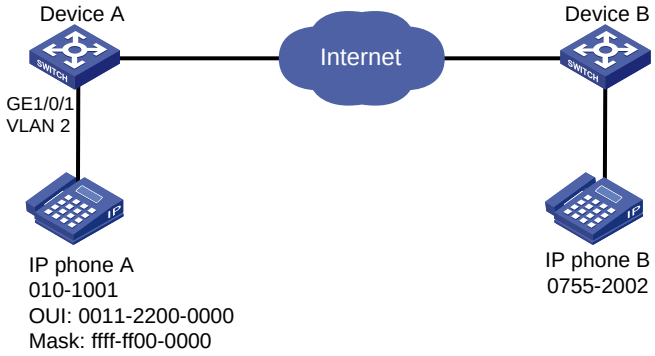
As shown in Figure 56:

- Device A transmits only voice traffic.
- IP phone A send untagged voice traffic.

For correct voice traffic transmission, perform the following tasks on Device A:

- Configure a voice VLAN to transmit voice traffic.
- Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.
- Add the MAC address of IP phone A to the device for voice packet identification. The mask is FFFF-FF00-0000.

Figure 56 Network diagram



Configuration procedure

Configure the voice VLAN to operate in security mode.

```
<DeviceA> system-view
[DeviceA] voice-vlan security enable
```

Add a MAC address 0011-2200-0000 with the mask FFFF-FF00-0000.

```
[DeviceA] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

Create VLAN 2.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

Configure VLAN 2 as the PVID of GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
```

Configure GigabitEthernet 1/0/1 to forward the voice traffic from VLAN 2 without VLAN tags.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

Enable voice VLAN and configure VLAN 2 as the voice VLAN on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan 2 enable
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the OUI addresses and their masks and descriptions.

```
[DeviceA] display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the voice VLAN state.

```
[DeviceA] display voice-vlan state
 Current Voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                            VLAN        Mode        CoS        DSCP
 GigabitEthernet1/0/1        2           Manual       6          46
```

Configuring MVRP

Multiple Registration Protocol (MRP) is an attribute registration protocol used to transmit attribute values.

Multiple VLAN Registration Protocol (MVRP) is a typical MRP application. It synchronizes VLAN information among devices.

MVRP propagates local VLAN information to other devices, receives VLAN information from other devices, and dynamically updates local VLAN information. When the network topology changes, MVRP propagates and learns VLAN information again according to the new topology.

MRP

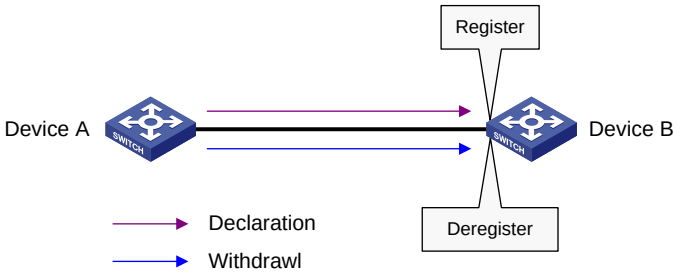
MRP allows devices in the same LAN to transmit attribute values on a per MSTI basis. For more information about MSTIs, see "Configuring spanning tree protocols."

MRP implementation

An MRP-enabled port is called an MRP participant. An MVRP-enabled port is called an MVRP participant.

As shown in Figure 57, an MRP participant sends declarations and withdrawals to notify other participants to register and deregister its attribute values. It also registers and deregisters the attribute values of other participants according to the received declarations and withdrawals. MRP rapidly propagates the configuration information of an MRP participant throughout the LAN.

Figure 57 MRP implementation



For example, MRP registers and deregisters VLAN attributes as follows:

- When a port receives a declaration for a VLAN, the port registers the VLAN and joins the VLAN.
- When a port receives a withdrawal for a VLAN, the port deregisters the VLAN and leaves the VLAN.

Figure 57 shows a simple MRP implementation on an MSTI. In a network with multiple MSTIs, MRP performs attribute registration and deregistration on a per-MSTI basis.

MRP messages

MRP messages include the following types:

- **Declaration**—Includes Join and New messages.
- **Withdrawal**—Includes Leave and LeaveAll messages.

Join message

An MRP participant sends a Join message to request the peer participant to register attributes in the Join message.

When receiving a Join message from the peer participant, an MRP participant performs the following tasks:

- Registers the attributes in the Join message.
- Propagates the Join message to all other participants on the device.

After receiving the Join message, other participants send the Join message to their respective peer participants.

Join messages sent from a local participant to its peer participant include the following types:

- **JoinEmpty**—Declares an unregistered attribute. For example, when an MRP participant joins an unregistered static VLAN, it sends a JoinEmpty message.

  VLANs created manually and locally are called static VLANs. VLANs learned through MRP are called dynamic VLANs.
- **JoinIn**—Declares a registered attribute. A JoinIn message is used in one of the following situations:
  - An MRP participant joins an existing static VLAN and sends a JoinIn message after registering the VLAN.
  - The MRP participant receives a Join message propagated by another participant on the device and sends a JoinIn message after registering the VLAN.

New message

Similar to a Join message, a New message enables MRP participants to register attributes.

When the MSTP topology changes, an MRP participant sends a New message to the peer participant to declare the topology change.

Upon receiving a New message from the peer participant, an MRP participant performs the following tasks:

- Registers the attributes in the message.
- Propagates the New message to all other participants on the device.

After receiving the New message, other participants send the New message to their respective peer participants.

Leave message

An MRP participant sends a Leave message to the peer participant when it wants the peer participant to deregister attributes that it has deregistered.

When the peer participant receives the Leave message, it performs the following tasks:

- Deregisters the attribute in the Leave message.
- Propagates the Leave message to all other participants on the device.

After a participant on the device receives the Leave message, it determines whether to send the Leave message to its peer participant depending on the attribute status on the device.

- If the VLAN in the Leave message is a dynamic VLAN not registered by any participants on the device, both of the following events occur:
  - The VLAN is deleted on the device.
  - The participant sends the Leave message to its peer participant.
- If the VLAN in the a Leave message is a static VLAN, the participant will not send the Leave message to its peer participant.

LeaveAll message

Each MRP participant starts its LeaveAll timer when starting up. When the timer expires, the MRP participant sends LeaveAll messages to the peer participant.

Upon sending or receiving a LeaveAll message, the local participant starts the Leave timer. The local participant determines whether to send a Join message depending on its the attribute status. A participant can re-register the attributes in the received Join message before the Leave timer expires.

When the Leave timer expires, a participant deregisters all attributes that have not been re-registered to periodically clear useless attributes in the network.

MRP timers

MRP uses the following timers to control message transmission.

Periodic timer

The Periodic timer controls the transmission of MRP messages. An MRP participant starts its own Periodic timer upon startup, and stores MRP messages to be sent before the Periodic timer expires. When the Periodic timer expires, MRP sends stored MRP messages in as few MRP frames as possible and restarts the Periodic timer. This mechanism reduces the number of MRP frames periodically sent.

You can enable or disable the Periodic timer. When the Periodic timer is disabled, MRP does not periodically send MRP messages. Instead, an MRP participant sends MRP messages when the LeaveAll timer expires or the participant receives a LeaveAll message from the peer participant.

Join timer

The Join timer controls the transmission of Join messages. An MRP participant starts the Join timer after sending a Join message to the peer participant. Before the Join timer expires, the participant does not resend the Join message when the following conditions exist:

- The participant receives a JoinIn message from the peer participant.
- The received JoinIn message has the same attributes as the sent Join message.

When both the Join timer and the Periodic timer expire, the participant resends the Join message.

Leave timer

The Leave timer controls the deregistration of attributes.

An MRP participant starts the Leave timer in one of the following conditions:

- The participant receives a Leave message from its peer participant.
- The participant receives or sends a LeaveAll message.

The MRP participant does not deregister the attributes in the Leave or LeaveAll message if the following conditions exist:

- The participant receives a Join message before the Leave timer expires.
- The Join message includes the attributes that have been encapsulated in the Leave or LeaveAll message.

If the participant does not receive a Join message for these attributes before the Leave timer expires, MRP deregisters the attributes.

LeaveAll timer

After startup, an MRP participant starts its own LeaveAll timer. When the LeaveAll timer expires, the MRP participant sends out a LeaveAll message and restarts the LeaveAll timer.

Upon receiving the LeaveAll message, other participants restart their LeaveAll timer. The value of the LeaveAll timer is randomly selected between the LeaveAll timer and 1.5 times the LeaveAll timer. This mechanism provides the following benefits:

- Effectively reduces the number of LeaveAll messages in the network.
- Prevents the LeaveAll timer of a particular participant from always expiring first.

MVRP registration modes

VLAN information propagated by MVRP includes dynamic VLAN information from other devices and local static VLAN information.

MVRP has the following registration modes, which process dynamic VLANs in different ways.

Normal

An MVRP participant in normal registration mode registers and deregisters dynamic VLANs.

Fixed

An MVRP participant in fixed registration mode disables deregistering dynamic VLANs and drops received MVRP frames. The MVRP participant does not deregister dynamic VLANs or register new dynamic VLANs.

Forbidden

An MVRP participant in forbidden registration mode disables registering dynamic VLANs and drops received MVRP frames. The MVRP participant does not register new dynamic VLANs or re-register a deregistered dynamic VLAN.

Protocols and standards

IEEE 802.1ak *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks – Amendment 07: Multiple Registration Protocol*

MVRP configuration task list

Tasks at a glance
(Required.) Enabling MVRP
(Optional.) Setting an MVRP registration mode
(Optional.) Setting MRP timers
(Optional.) Enabling GVRP compatibility

Configuration restrictions and guidelines

When you configure MVRP, follow these restrictions and guidelines:

- MVRP can work with STP, RSTP, or MSTP. MVRP cannot work with other link layer topology protocols, including service loopback, PVST, RRPP, and Smart Link. Ports blocked by STP, RSTP, or MSTP can receive and send MVRP frames.

  For more information about STP, RSTP, MSTP, and PVST, see "Configuring spanning tree protocols."

  For more information about service loopback, see "Configuring service loopback groups."

For more information about RRPP and Smart Link, see *High Availability Configuration Guide*.

- Do not configure both MVRP and remote port mirroring on a port. Otherwise, MVRP might register the remote probe VLAN with incorrect ports, which would cause the monitor port to receive undesired copies. For more information about port mirroring, see *Network Management and Monitoring Configuration Guide*.
- MVRP takes effect only on trunk ports. For more information about trunk ports, see "Configuring VLANs."
- Enabling MVRP on a Layer 2 aggregate interface takes effect on the aggregate interface and all Selected member ports in the link aggregation group.
- MVRP configuration made on an aggregation group member port takes effect only after the port is removed from the aggregation group.

Configuration prerequisites

Before configuring MVRP, make sure each MSTI is mapped to an existing VLAN on each device in the network.

Enabling MVRP

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MVRP globally.	**mvrp global enable**	By default, MVRP is globally disabled. To make MVRP take effect on a port, enable MVRP both on the port and globally.
3. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the port as a trunk port.	**port link-type trunk**	By default, any port is an access port. For more information about the **port link-type trunk** command, see *Layer 2—LAN Switching Command Reference*.
5. Configure the trunk port to permit the specified VLANs.	**port trunk permit vlan** { *vlan-id-list* | **all** }	By default, a trunk port permits only VLAN 1. Make sure the trunk port permits all registered VLANs. For more information about the **port trunk permit vlan** command, see *Layer 2—LAN Switching Command Reference*.
6. Enable MVRP on the port.	**mvrp enable**	By default, MVRP is disabled on a port.

Setting an MVRP registration mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Set an MVRP registration mode.	**mvrp registration** { **fixed** | **forbidden** | **normal** }	Optional. The default setting is normal registration mode.

Setting MRP timers

To avoid frequent VLAN registrations and deregistrations, use the same MRP timers throughout the network.

Each port maintains its own Periodic, Join, and LeaveAll timers, and each attribute of a port maintains a Leave timer.

To set MRP timers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Set the LeaveAll timer.	**mrp timer leaveall** *timer-value*	Optional. The default setting is 1000 centiseconds.
4. Set the Join timer.	**mrp timer join** *timer-value*	Optional. The default setting is 20 centiseconds.
5. Set the Leave timer.	**mrp timer leave** *timer-value*	Optional. The default setting is 60 centiseconds.
6. Set the Periodic timer.	**mrp timer periodic** *timer-value*	Optional. The default setting is 100 centiseconds. You can restore the Periodic timer to the default at any time.

Table 15 shows the value ranges for Join, Leave, and LeaveAll timers and their dependencies.

- If you set a timer to a value beyond the allowed value range, your configuration fails. You can set a timer by tuning the value of any other timer. The value of each timer must be an integer multiple of 20 centiseconds and in the range defined in Table 15.
- As a best practice, restore the timers in the order of Join, Leave, and LeaveAll when you restore the default settings for the timers.

Table 15 Dependencies of the Join, Leave, and LeaveAll timers

Timer	Lower limit	Upper limit
Join	20 centiseconds	Half the Leave timer
Leave	Twice the Join timer	LeaveAll timer
LeaveAll	Leave timer on each port	32760 centiseconds

Enabling GVRP compatibility

Enable GVRP compatibility for MVRP when the peer device supports GVRP. Then, the local end can receive and send both MVRP and GVRP frames.

When you enable GVRP compatibility, follow these restrictions and guidelines:

- GVRP compatibility enables MVRP to work with STP or RSTP, but not MSTP.
- When the system is busy, disable the Period timer to prevent the participant from frequently registering or deregistering attributes.

To enable GVRP compatibility:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable GVRP compatibility.	**mvrp gvrp-compliance enable**	By default, GVRP compatibility is disabled.

Displaying and maintaining MVRP

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display MVRP running status.	**display mvrp running-status** [**interface** *interface-list*]
Display the MVRP state of a port in a VLAN.	**display mvrp state interface** *interface-type interface-number* **vlan** vlan-id
Display MVRP statistics.	**display mvrp statistics** [**interface** *interface-list*]
Clear MVRP statistics.	**reset mvrp statistics** [**interface** *interface-list*]

MVRP configuration example

Network requirements

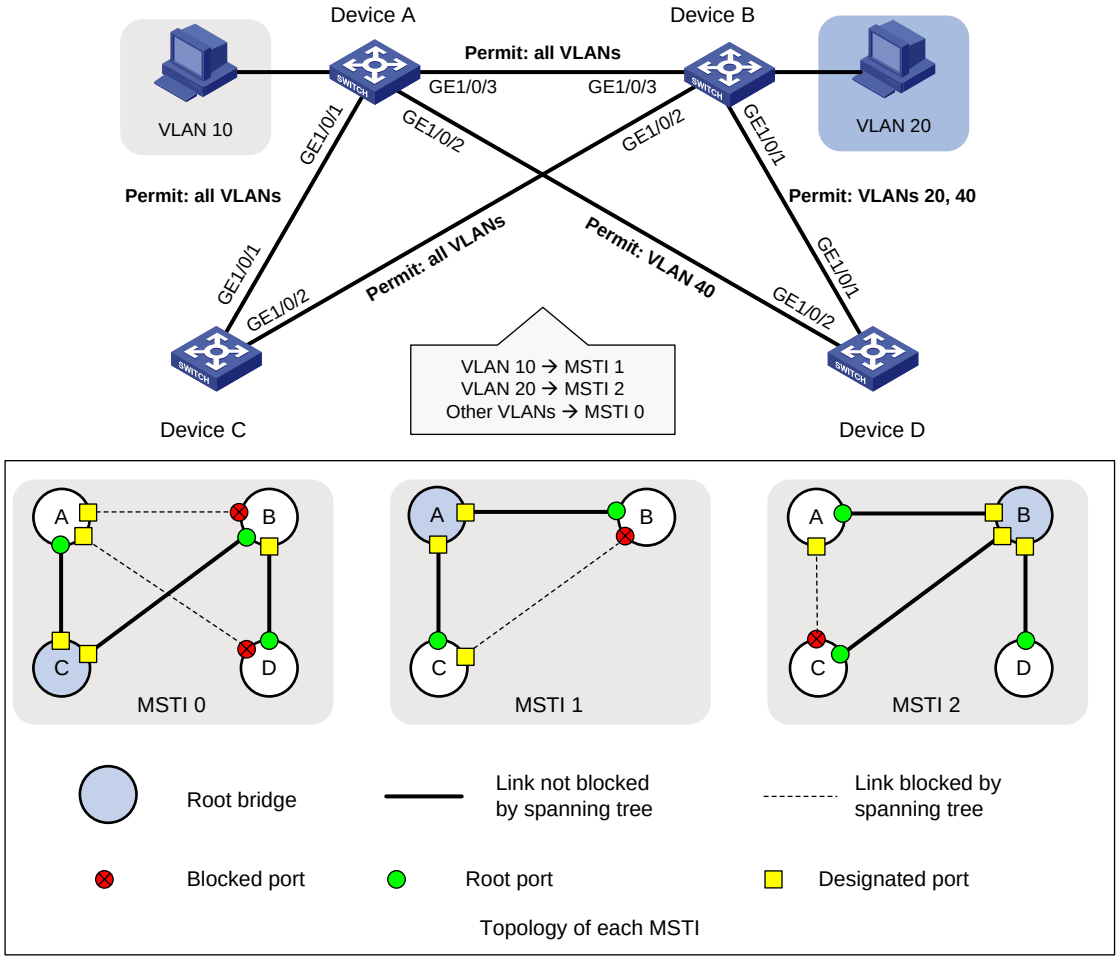
As shown in Figure 58:

- Create VLAN 10 on Device A and VLAN 20 on Device B.
- Configure MSTP, map VLAN 10 to MSTI 1, map VLAN 20 to MSTI 2, and map the other VLANs to MSTI 0.

Configure MVRP on Device A, Device B, Device C, and Device D to meet the following requirements:

- The devices can register and deregister dynamic VLANs.
- The devices can keep identical VLAN configuration for each MSTI.

Figure 58 Network diagram



Configuration procedure

1. Configure Device A:

   # Enter MST region view.

   ```
   <DeviceA> system-view
   [DeviceA] stp region-configuration
   ```

   # Configure the MST region name, VLAN-to-instance mappings, and revision level.

   ```
   [DeviceA-mst-region] region-name example
   [DeviceA-mst-region] instance 1 vlan 10
   [DeviceA-mst-region] instance 2 vlan 20
   [DeviceA-mst-region] revision-level 0
   ```

   # Manually activate the MST region configuration.

   ```
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   ```

   # Configure Device A as the primary root bridge of MSTI 1.

   ```
   [DeviceA] stp instance 1 root primary
   ```

Globally enable the spanning tree feature.

```
[DeviceA] stp global enable
```

Globally enable MVRP.

```
[DeviceA] mvrp global enable
```

Configure GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] mvrp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and configure it to permit VLAN 40.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 40
```

Enable MVRP on port GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] mvrp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan all
```

Enable MVRP on GigabitEthernet 1/0/3.

```
[DeviceA-GigabitEthernet1/0/3] mvrp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

Create VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

2. Configure Device B:

Enter MST region view.

```
<DeviceB> system-view
[DeviceB] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 2 vlan 20
[DeviceB-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure Device B as the primary root bridge of MSTI 2.

```
[DeviceB] stp instance 2 root primary
```

Globally enable the spanning tree feature.

```
[DeviceB] stp global enable
```

Globally enable MVRP.

```
[DeviceB] mvrp global enable
```

Configure GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```

Enable MVRP on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] mvrp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and configure it to permit all VLANs.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan all
```

Enable MVRP on GigabitEthernet 1/0/2.

```
[DeviceB-GigabitEthernet1/0/2] mvrp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan all
```

Enable MVRP on GigabitEthernet 1/0/3.

```
[DeviceB-GigabitEthernet1/0/3] mvrp enable
[DeviceB-GigabitEthernet1/0/3] quit
```

Create VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

3. Configure Device C:

Enter MST region view.

```
<DeviceC> system-view
[DeviceC] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 2 vlan 20
[DeviceC-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Configure Device C as the root bridge of MSTI 0.

```
[DeviceC] stp instance 0 root primary
```

Globally enable the spanning tree feature.

```
[DeviceC] stp global enable
```

Globally enable MVRP.

```
[DeviceC] mvrp global enable
```

Configure GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable MVRP on GigabitEthernet 1/0/1.

```
[DeviceC-GigabitEthernet1/0/1] mvrp enable
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and configure it to permit all VLANs.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan all
```

Enable MVRP on GigabitEthernet 1/0/2.

```
[DeviceC-GigabitEthernet1/0/2] mvrp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

4. Configure Device D:

Enter MST region view.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 2 vlan 20
[DeviceD-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Globally enable the spanning tree feature.

```
[DeviceD] stp global enable
```

Globally enable MVRP.

```
[DeviceD] mvrp global enable
```

Configure GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```

Enable MVRP on GigabitEthernet 1/0/1.

```
[DeviceD-GigabitEthernet1/0/1] mvrp enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and configure it to permit VLAN 40.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 40
```

Enable MVRP on GigabitEthernet 1/0/2.

```
[DeviceD-GigabitEthernet1/0/2] mvrp enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verifying the normal registration mode configuration

Display the local VLAN information on Device A.

```
[DeviceA] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False
```

```
----[GigabitEthernet1/0/1]----
Config  Status                 : Enabled
Running Status                 : Enabled
Join Timer                     : 20 (centiseconds)
Leave Timer                    : 60 (centiseconds)
Periodic Timer                 : 100 (centiseconds)
LeaveAll Timer                 : 1000 (centiseconds)
Registration Type              : Normal
Registered VLANs :
 1(default)
Declared VLANs :
 1(default), 10, 20
Propagated VLANs :
 1(default)

----[GigabitEthernet1/0/2]----
Config  Status                 : Enabled
Running Status                 : Enabled
Join Timer                     : 20 (centiseconds)
Leave Timer                    : 60 (centiseconds)
Periodic Timer                 : 100 (centiseconds)
LeaveAll Timer                 : 1000 (centiseconds)
Registration Type              : Normal
Registered VLANs :
 None
Declared VLANs :
 1(default)
Propagated VLANs :
 None

----[GigabitEthernet1/0/3]----
Config  Status                 : Enabled
Running Status                 : Enabled
Join Timer                     : 20 (centiseconds)
Leave Timer                    : 60 (centiseconds)
Periodic Timer                 : 100 (centiseconds)
LeaveAll Timer                 : 1000 (centiseconds)
Registration Type              : Normal
Registered VLANs :
 20
Declared  VLANs :
 1(default), 10
Propagated VLANs :
 20
```

The output shows that the following events have occurred:

- GigabitEthernet 1/0/1 has registered VLAN 1, declared VLAN 1, VLAN 10, and VLAN 20, and propagated VLAN 1 through MVRP.

- GigabitEthernet 1/0/2 has declared VLAN 1, and registered and propagated no VLANs.
- GigabitEthernet 1/0/3 has registered VLAN 20, declared VLAN 1 and VLAN 10, and propagated VLAN 20 through MVRP.

Display the local VLAN information on Device B.

```
[DeviceB] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default)
 Declared VLANs :
  1(default), 20
 Propagated VLANs :
  1(default)

 ----[GigabitEthernet1/0/2]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 10
 Declared VLANs :
  1(default), 20
 Propagated VLANs :
  1(default)

 ----[GigabitEthernet1/0/3]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
```

```
 1(default), 10
Declared VLANs :
 20
Propagated VLANs :
 10
```

The output shows that the following events have occurred:

- GigabitEthernet 1/0/1 has registered VLAN 1, declared VLAN 1 and VLAN 20, and propagated VLAN 1 through MVRP.
- GigabitEthernet 1/0/2 has registered VLAN 1 and VLAN 10, declared VLAN 1 and VLAN 20, and propagated VLAN 1.
- GigabitEthernet 1/0/3 has registered VLAN 1 and VLAN 10, declared VLAN 20, and propagated VLAN 10 through MVRP.

Display the local VLAN information on Device C.

```
[DeviceC] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 10, 20
 Declared VLANs :
  1(default)
 Propagated VLANs :
  1(default), 10

 ----[GigabitEthernet1/0/2]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 20
 Declared VLANs :
  1(default), 10
 Propagated VLANs :
  1(default), 20
```

The output shows that the following events have occurred:

- GigabitEthernet 1/0/1 has registered VLAN 1, VLAN 10, and VLAN 20, declared VLAN 1, and propagated VLAN 1 and VLAN 10 through MVRP.
- GigabitEthernet 1/0/2 has registered VLAN 1 and VLAN 20, declared VLAN 1 and VLAN 10, and propagated VLAN 1 and VLAN 20 through MVRP.

Display the local VLAN information on Device D.

```
[DeviceD] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 20
 Declared VLANs :
  1(default)
 Propagated VLANs :
  1(default), 20

 ----[GigabitEthernet1/0/2]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default)
 Declared  VLANs :
  None
 Propagated VLANs :
  None
```

The output shows that the following events have occurred:

- GigabitEthernet 1/0/1 has registered and propagated VLAN 10 and VLAN 20, and declared VLAN 1 through MVRP.
- Port GigabitEthernet 1/0/2 has registered VLAN 1, and declared and propagated no VLANs through MVRP.

Verifying the configuration after changing the registration mode

When the network is stable, set the MVRP registration mode to **fixed** on the port of Device B connected to Device A. Then, verify that dynamic VLANs on the port will not be deregistered.

Set the MVRP registration mode to **fixed** on GigabitEthernet 1/0/3 of Device B.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] mvrp registration fixed
[DeviceB-GigabitEthernet1/0/3] quit
```

Display the local MVRP VLAN information on GigabitEthernet 1/0/3 of Device B.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/3]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Fixed
 Registered VLANs :
  1(default), 10
 Declared VLANs :
  20
 Propagated VLANs :
  10
```

The output shows that VLAN information on GigabitEthernet 1/0/3 is not changed after you set its MVRP registration mode to **fixed**.

Delete VLAN 10 on Device A.

```
[DeviceA] undo vlan 10
```

Display the local MVRP VLAN information on GigabitEthernet 1/0/3 of Device B.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/3]----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Fixed
 Registered VLANs :
  1(default), 10
 Declared VLANs :
  20
 Propagated VLANs :
  10
```

The output shows that the dynamic VLAN information on GigabitEthernet 1/0/3 is not changed after you set its MVRP registration mode to **fixed**.

Configuring QinQ

This document uses the following terms:

- **CVLAN**—Customer network VLANs, also called inner VLANs, refer to VLANs that a customer uses on the private network.
- **SVLAN**—Service provider network VLANs, also called outer VLANs, refer to VLANs that a service provider uses to transmit VLAN tagged traffic for customers.

Overview

802.1Q-in-802.1Q (QinQ) adds an 802.1Q tag to 802.1Q tagged customer traffic. It enables a service provider to extend Layer 2 connections across an Ethernet network between customer sites.

QinQ provides the following benefits:

- Enables a service provider to use a single SVLAN to convey multiple CVLANs for a customer.
- Enables customers to plan CVLANs without conflicting with SVLANs.
- Enables customers to keep their VLAN assignment schemes unchanged when the service provider changes its VLAN assignment scheme.
- Allows customers to use overlapping CVLAN IDs. Devices in the service provider network make forwarding decisions based on SVLAN IDs instead of CVLAN IDs.

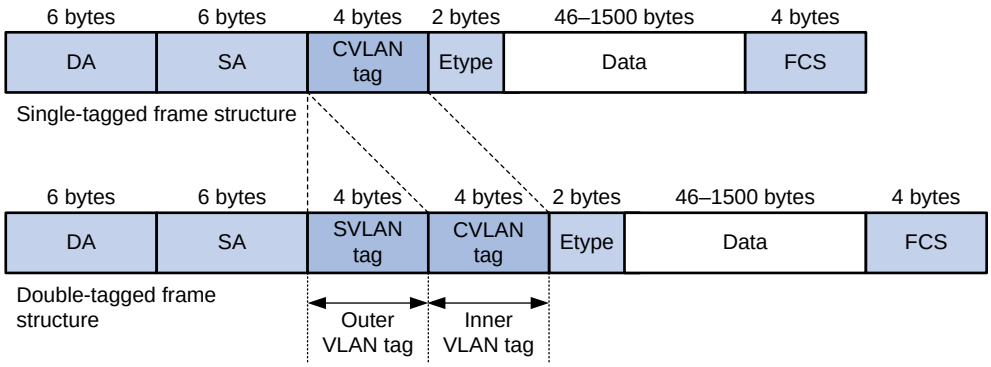
How QinQ works

As shown in Figure 59, a QinQ frame transmitted over the service provider network carries the following tags:

- **CVLAN tag**—Identifies the VLAN to which the frame belongs when it is transmitted in the customer network.
- **SVLAN tag**—Identifies the VLAN to which the QinQ frame belongs when it is transmitted in the service provider network. The service provider allocates the SVLAN tag to the customer.

The devices in the service provider network forward a tagged frame based on its SVLAN tag. The CVLAN tag is transmitted as part of the frame's payload.

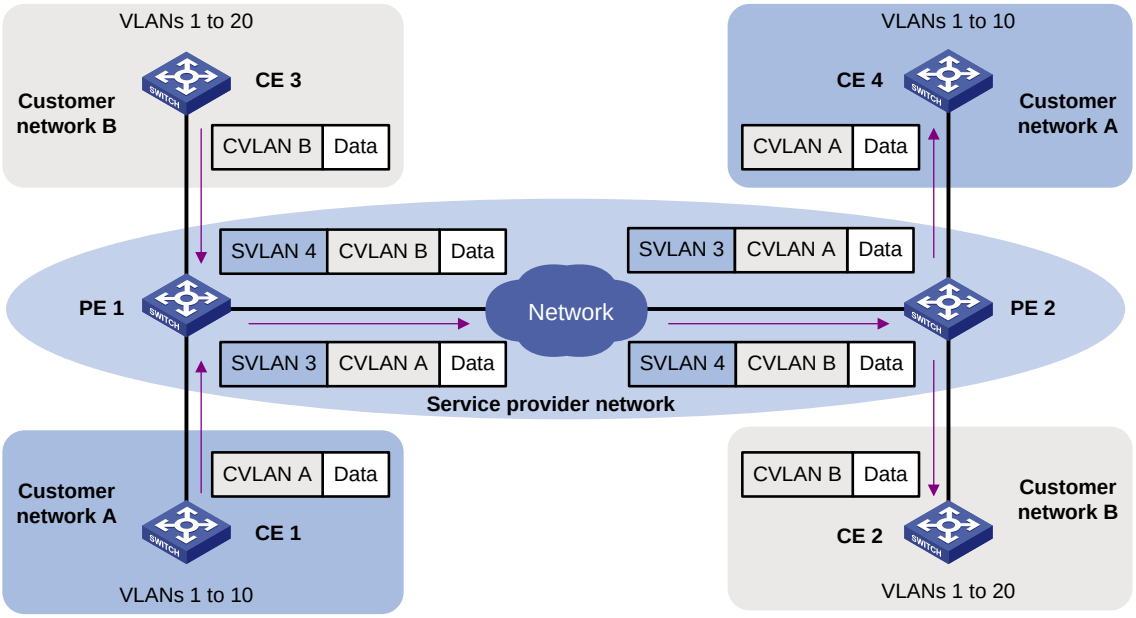
Figure 59 Single-tagged Ethernet frame header and double-tagged Ethernet frame header



As shown in Figure 60, customer A has remote sites CE 1 and CE 4. Customer B has remote sites CE 2 and CE 3. The CVLANs of the two customers overlap. The service provider assigns SVLANs 3 and 4 to customers A and B, respectively.

When a tagged frame from CE 1 arrives, PE 1 tags the frame with SVLAN 3. The double-tagged frame travels over the service provider network until it arrives at PE 2. PE 2 removes the SVLAN tag of the frame, and then sends the frame to CE 4.

Figure 60 Typical QinQ application scenario



QinQ implementations

QinQ is enabled on a per-port basis. The link type of a QinQ-enabled port can be access, hybrid, or trunk. The QinQ tagging behaviors are the same across these types of ports.

A QinQ-enabled port tags all incoming frames (tagged or untagged) with the PVID tag.

- If an incoming frame already has one tag, it becomes a double-tagged frame.
- If the frame does not have any 802.1Q tags, it becomes a frame tagged with the PVID.

QinQ provides the most basic VLAN manipulation method to tag all incoming frames (tagged or untagged) with the PVID tag. To perform advanced VLAN manipulations, use VLAN mapping (see "Configuring VLAN mapping") or QoS policies. For example:

- To use different SVLANs for different CVLAN tags, use one-to-two VLAN mapping.
- To replace the SVLAN ID, CVLAN ID, or both IDs for an incoming double-tagged frame, use two-to-two VLAN mapping.
- To set the 802.1p priority in SVLAN tags, configure a QoS policy as described in "Setting the 802.1p priority in SVLAN tags."

Protocols and standards

- IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks*
- IEEE 802.1ad, *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks-Amendment 4: Provider Bridges*

Restrictions and guidelines

When you configure QinQ, follow these restrictions and guidelines:

- Before you configure QinQ on a port, you must remove all VLAN mappings on the port. After you enable QinQ on the port, you can configure any VLAN mapping types except two-to-two VLAN mapping on it. If QinQ and a VLAN mapping conflict, the VLAN mapping takes effect.
- The inner 802.1Q tag of QinQ frames is treated as part of the payload. As a best practice to ensure correct transmission of QinQ frames, set the MTU to a minimum of 1504 bytes for each port on the forwarding path of QinQ frames. This value is the sum of the default Ethernet interface MTU (1500 bytes) and the length (4 bytes) of a VLAN tag.

Enabling QinQ

Enable QinQ on customer-side ports of PEs. A QinQ-enabled port tags an incoming frame with its PVID.

To enable QinQ:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable QinQ.	**qinq enable**	By default, QinQ is disabled.

Configuring transparent transmission for VLANs

You can exclude traffic of a VLAN (for example, the management VLAN) from the QinQ tagging action on a customer-side port. This VLAN is called a transparent VLAN.

To ensure successful transmission for a transparent VLAN, follow these configuration guidelines:

- Set the link type of the port to trunk or hybrid, and assign the port to its PVID and the transparent VLAN.
- Do not configure any other VLAN manipulation actions for the VLAN on the port.
- Make sure all ports on the traffic path permit the VLAN to pass through.

To enable transparent transmission for a list of VLANs:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the port link type.	**port link-type** { **hybrid** | **trunk** }	By default, the link type of ports is access.
4. Configure the port to allow packets from its PVID and the transparent VLANs to pass through.	• For hybrid ports: **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } • For trunk ports: **port trunk permit vlan**	By default, trunk ports allow only packets from VLAN 1 to pass through. Hybrid ports allow only packets from VLAN 1 to pass through

Step	Command	Remarks
	{ *vlan-id-list* | **all** }	untagged.
5. Enable QinQ on the port.	**qinq enable**	By default, QinQ is disabled.
6. Specify transparent VLANs.	**qinq transparent-vlan** *vlan-list*	By default, transparent transmission is not configured for any VLANs on a port.

Configuring the TPID in VLAN tags

TPID identifies a frame as an 802.1Q tagged frame. The TPID value varies by vendor. On the device, the TPID in the 802.1Q tag added on a QinQ-enabled port is 0x8100 by default, in compliance with IEEE 802.1Q. In a multi-vendor network, make sure the TPID setting is the same across all devices so 802.1Q tagged frames can be identified correctly.

TPID settings include CVLAN TPID and SVLAN TPID.

A QinQ-enabled port uses the CLAN TPID to match incoming tagged frames. An incoming frame is handled as untagged if its TPID is different from the CVLAN TPID.

SVLAN TPIDs are configurable on a per-port basis. A service provider-side port uses the SVLAN TPID to replace the TPID in outgoing frames' SVLAN tags and match incoming tagged frames. An incoming frame is handled as untagged if the TPID in its outer VLAN tag is different from the SVLAN TPID.

For example, a PE device is connected to a customer device that uses the TPID 0x8200 and to a provider device that uses the TPID 0x9100. For correct packet processing, you must set the CVLAN TPID and SVLAN TPID to 0x8200 and 0x9100 on the PE, respectively.

The TPID field is in the same position as the EtherType field in an untagged Ethernet frame. To ensure correct packet type identification, do not set the TPID value to any of the values listed in Table 16.

Table 16 Reserved EtherType values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E
LLDP	0x88CC
802.1ag	0x8902
Cluster	0x88A7

Protocol type	Value
Reserved	0xFFFD/0xFFFE/0xFFFF

Configuring the CVLAN TPID

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the TPID value for CVLAN tags.	**qinq ethernet-type customer-tag** *hex-value*	The default setting is 0x8100 for CVLAN tags.

Configuring the SVLAN TPID

When you configure the SVLAN ID, follow these restrictions and guidelines:

- Configure the SVLAN TPID on service provider-side ports of PEs.
- Do not configure the SVLAN TPID on a QinQ-enabled port.

To configure the SVLAN TPID:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view or aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the SVLAN TPID.	**qinq ethernet-type service-tag** *hex-value*	The default setting is 0x8100 for SVLAN tags.

Setting the 802.1p priority in SVLAN tags

By default, a QinQ-enabled port sets the 802.1p priority in the SVLAN tag depending on the priority trust mode.

- If the 802.1p priority is trusted, the port copies the 802.1p priority in the CVLAN tag to the SVLAN tag.
- If port priority is trusted, the port sets the 802.1p priority in the SVLAN to be the same as the port priority. The default port priority is 0.

Alternatively, you can configure a QoS policy to set the 802.1p priority in the SVLAN by using one of the following methods:

- Sets an 802.1p priority value in the SVLAN tag depending on the VLAN ID or 802.1p priority in the CVLAN tag.
- Copies the 802.1p priority in the CVLAN tag to the SVLAN tag.

To set the 802.1p priority in SVLAN tags:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic class and enter traffic class view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic class is configured.

Step	Command	Remarks
3. Configure CVLAN match criteria.	• Match CVLAN IDs: **if-match customer-vlan-id** *vlan-id-list* • Match 802.1p priority: **if-match customer-dot1p** *dot1p-value*&<1-8>	N/A
4. Return to system view.	**quit**	N/A
5. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	N/A
6. Configure a priority marking action for SVLAN tags.	• Replace the priority in the SVLAN tags of matching frames with the configured priority: **remark dot1p** *dot1p-value* • Copy the 802.1p priority in the CVLAN tag to the SVLAN tag: **remark dot1p customer-dot1p-trust**	N/A
7. Return to system view.	**quit**	N/A
8. Create a QoS policy and enter QoS policy view.	**qos policy** *policy-name*	N/A
9. Associate the traffic class with the traffic behavior.	**classifier** *classifier-name* **behavior** *behavior-name*	N/A
10. Return to system view.	**quit**	N/A
11. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
12. Configure the port to trust the 802.1p priority in incoming frames.	**qos trust dot1p**	By default, the device does not trust the 802.1p priority carried in frames. Skip this step if the **remark dot1p customer-dot1p-trust** command is configured.
13. Enable QinQ.	**qinq enable**	N/A
14. Apply the QoS policy to the inbound direction of the port.	**qos apply policy** *policy-name* **inbound**	N/A

For more information about QoS policies, see *ACL and QoS Configuration Guide*.

Displaying and maintaining QinQ

Execute **display** commands in any view.

Task	Command
Display QinQ-enabled ports.	**display qinq** [**interface** *interface-type interface-number*]

QinQ configuration examples

Basic QinQ configuration example

Network requirements

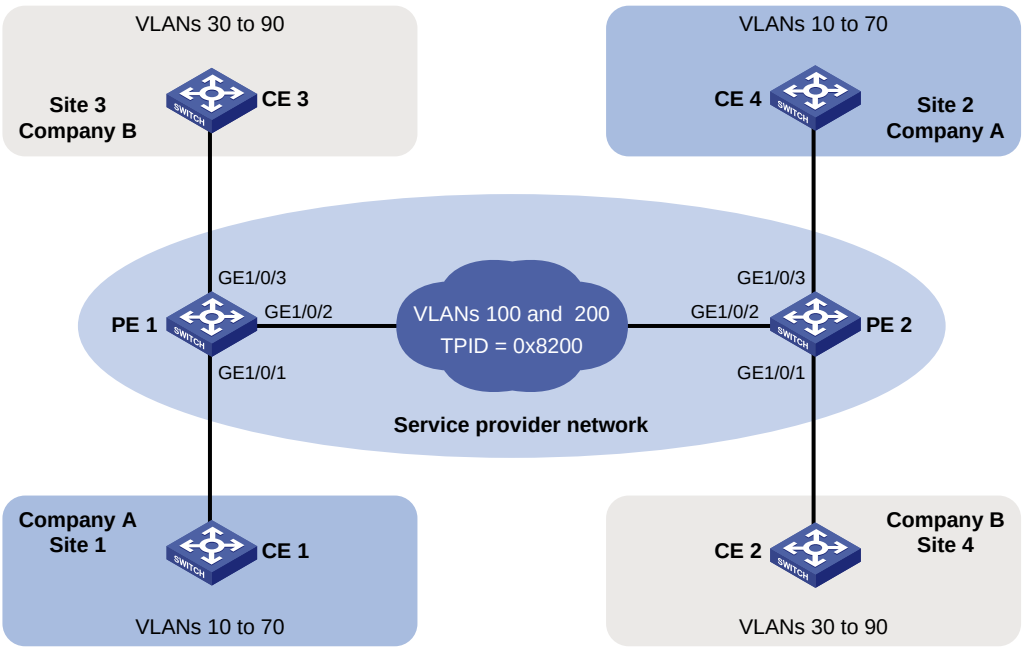
As shown in Figure 61:

- The service provider assigns VLAN 100 to Company A's VLANs 10 through 70.
- The service provider assigns VLAN 200 to Company B's VLANs 30 through 90.
- The devices between PE 1 and PE 2 in the service provider network use a TPID value of 0x8200.

Configure QinQ on PE 1 and PE 2 to transmit traffic in VLANs 100 and 200 for Company A and Company B, respectively.

For the QinQ frames to be identified correctly, set the SVLAN TPID to 0x8200 on the service provider-side ports of PE 1 and PE 2.

Figure 61 Network diagram



Configuration procedure

1. Configure PE 1:

   # Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 100.

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Configure VLAN 100 as the PVID for GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

Enable QinQ on GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qinq enable
[PE1-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 200.

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Set the TPID value in the SVLAN tags to 0x8200 on GigabitEthernet 1/0/2.

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 200.

```
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] port link-type trunk
[PE1-GigabitEthernet1/0/3] port trunk permit vlan 200
```

Configure VLAN 200 as the PVID for GigabitEthernet 1/0/3.

```
[PE1-GigabitEthernet1/0/3] port trunk pvid vlan 200
```

Enable QinQ on GigabitEthernet 1/0/3.

```
[PE1-GigabitEthernet1/0/3] qinq enable
[PE1-GigabitEthernet1/0/3] quit
```

2. Configure PE 2:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 200.

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 200
```

Configure VLAN 200 as the PVID for GigabitEthernet 1/0/1.

```
[PE2-GigabitEthernet1/0/1] port trunk pvid vlan 200
```

Enable QinQ on GigabitEthernet 1/0/1.

```
[PE2-GigabitEthernet1/0/1] qinq enable
[PE2-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 200.

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Set the TPID value in the SVLAN tags to 0x8200 on GigabitEthernet 1/0/2.

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 100.

```
[PE2] interface gigabitethernet 1/0/3
[PE2-GigabitEthernet1/0/3] port link-type trunk
[PE2-GigabitEthernet1/0/3] port trunk permit vlan 100
```

Configure VLAN 100 as the PVID for GigabitEthernet 1/0/3.

```
[PE2-GigabitEthernet1/0/3] port trunk pvid vlan 100
```

Enable QinQ on GigabitEthernet 1/0/3.

```
[PE2-GigabitEthernet1/0/3] qinq enable
```

```
[PE2-GigabitEthernet1/0/3] quit
```

3. Configure the devices between PE 1 and PE 2:

   # Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. (Details not shown.)

   # Configure all the ports on the forwarding path to allow frames from VLANs 100 and 200 to pass through without removing the VLAN tag. (Details not shown.)

VLAN transparent transmission configuration example

Network requirements

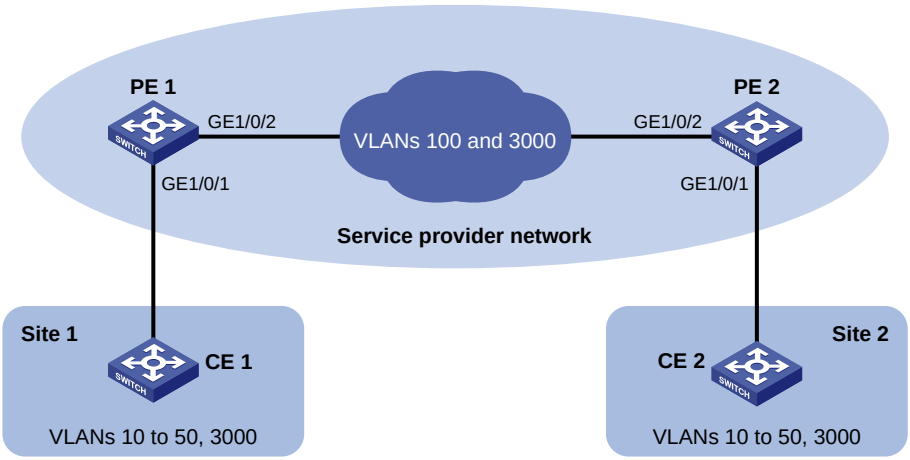
As shown in Figure 62:

- The service provider assigns VLAN 100 to a company's VLANs 10 through 50.
- VLAN 3000 is the dedicated VLAN of the company on the service provider network.

Configure QinQ on PE 1 and PE 2 to provide Layer 2 connectivity for CVLANs 10 through 50 over the service provider network.

Configure VLAN transparent transmission for VLAN 3000 on PE 1 and PE 2 to enable the hosts in VLAN 3000 to communicate without using an SVLAN.

Figure 62 Network diagram



Configuration procedure

1. Configure PE 1:

   # Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 100 and 3000.

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 100 3000
```

   # Configure VLAN 100 as the PVID of GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

   # Enable QinQ on GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

   # Configure GigabitEthernet 1/0/1 to transparently transmit frames from VLAN 3000.

```
[PE1-GigabitEthernet1/0/1] qinq transparent-vlan 3000
[PE1-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 3000.

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 3000
[PE1-GigabitEthernet1/0/2] quit
```

2. Configure PE 2:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 100 and 3000.

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100 3000
```

Configure VLAN 100 as the PVID of GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

Enable QinQ on GigabitEthernet 1/0/1.

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

Configure GigabitEthernet 1/0/1 to transparently transmit frames from VLAN 3000.

```
[PE2-GigabitEthernet1/0/1] qinq transparent-vlan 3000
[PE2-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 3000.

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 3000
```

3. Configure the devices between PE 1 and PE 2:

Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. (Details not shown.)

Configure all the ports on the forwarding path to allow frames from VLANs 100 and 3000 to pass through without removing the VLAN tag. (Details not shown.)

Configuring VLAN mapping

Overview

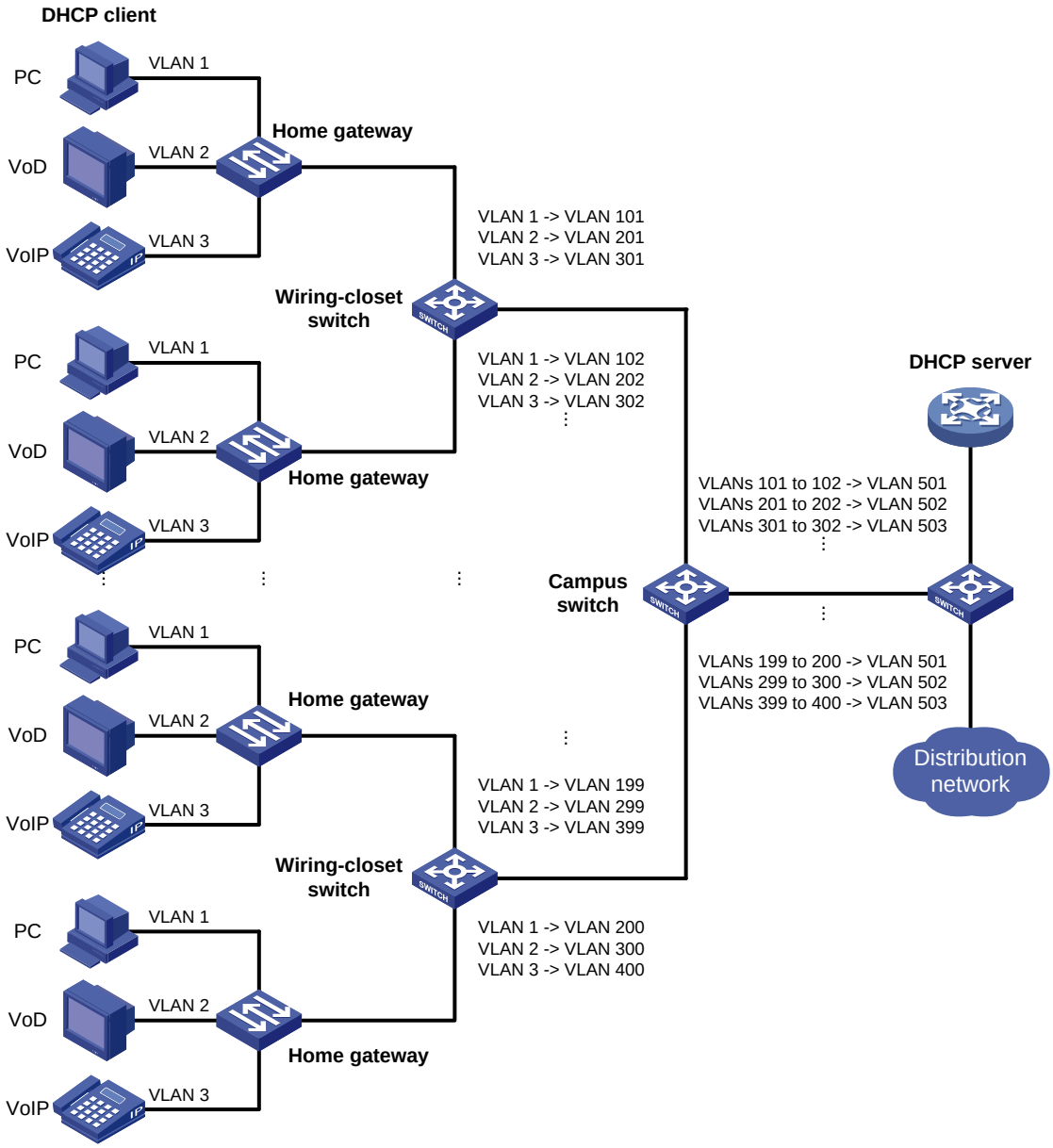
VLAN mapping re-marks VLAN tagged traffic with new VLAN IDs. Hewlett Packard Enterprise provides the following types of VLAN mapping:

- **One-to-one VLAN mapping**—Replaces one VLAN tag with another.
- **Many-to-one VLAN mapping**—Replaces multiple VLAN tags with the same VLAN tag.
- **One-to-two VLAN mapping**—Tags single-tagged packets with an outer VLAN tag.
- **Two-to-two VLAN mapping**—Replaces the SVLAN ID, CVLAN ID, or both IDs for an incoming double-tagged frame.

Application scenario of one-to-one and many-to-one VLAN mapping

Figure 63 shows a typical application scenario of one-to-one and many-to-one VLAN mapping. The scenario implements broadband Internet access for a community.

Figure 63 Application scenario of one-to-one and many-to-one VLAN mapping



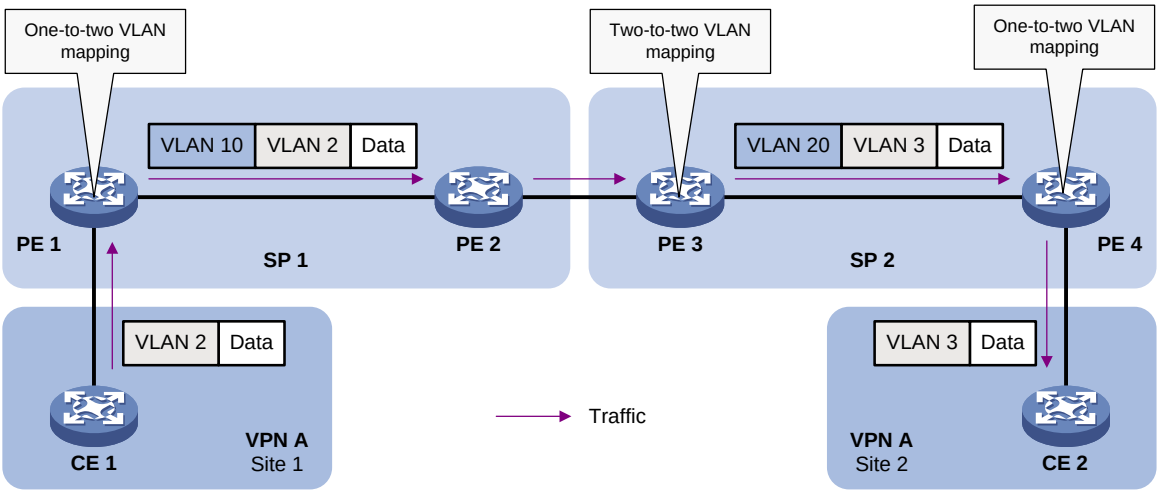
As shown in Figure 63, the network is implemented as follows:

- Each home gateway uses different VLANs to transmit the PC, VoD, and VoIP services.
- To further subclassify each type of traffic by customer, configure one-to-one VLAN mapping on the wiring-closet switches. This feature assigns a separate VLAN to each type of traffic from each customer. The required total number of VLANs in the network can be very large.
- To prevent the maximum number of VLANs from being exceeded on the distribution layer device, configure many-to-one VLAN mapping on the campus switch. This feature assigns the same VLAN to the same type of traffic from different customers.

Application scenario of one-to-two and two-to-two VLAN mapping

Figure 64 shows a typical application scenario of one-to-two and two-to-two VLAN mapping. In this scenario, the remote sites of the same VPN must communicate across two SP networks.

Figure 64 Application scenario of one-to-two and two-to-two VLAN mapping



Site 1 and Site 2 are in VLAN 2 and VLAN 3, respectively. The SP 1 network assigns SVLAN 10 to Site 1. The SP 2 network assigns SVLAN 20 to Site 2. When the packet from Site 1 arrives at PE 1, PE 1 tags the packet with SVLAN 10 by using one-to-two VLAN mapping.

When the double-tagged packet from the SP 1 network arrives at the SP 2 network interface, PE 3 processes the packet as follows:

- Replaces SVLAN tag 10 with SVLAN tag 20.
- Replaces CVLAN tag 2 with CVLAN tag 3.

One-to-two VLAN mapping provides the following benefits:

- Enables a customer network to plan its CVLAN assignment without conflicting with SVLANs.
- Adds a VLAN tag to a tagged packet and expands the number of available VLANs to 4094 × 4094.
- Reduces the stress on the SVLAN resources, which were 4094 VLANs in the SP network before the mapping process was initiated.

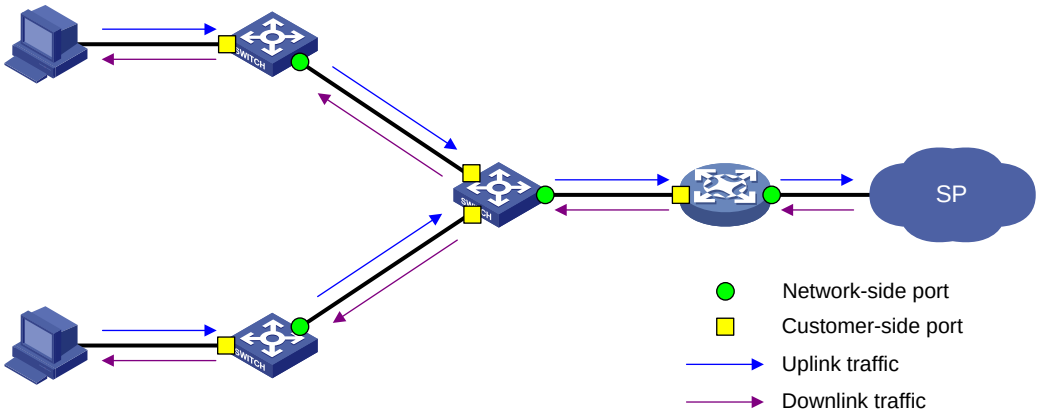
VLAN mapping implementations

Figure 65 shows a simplified network that illustrates basic VLAN mapping terms.

Basic VLAN mapping terms include the following:

- **Uplink traffic**—Traffic transmitted from the customer network to the service provider network.
- **Downlink traffic**—Traffic transmitted from the service provider network to the customer network.
- **Network-side port**—A port connected to or closer to the service provider network.
- **Customer-side port**—A port connected to or closer to the customer network.

Figure 65 Basic VLAN mapping terms

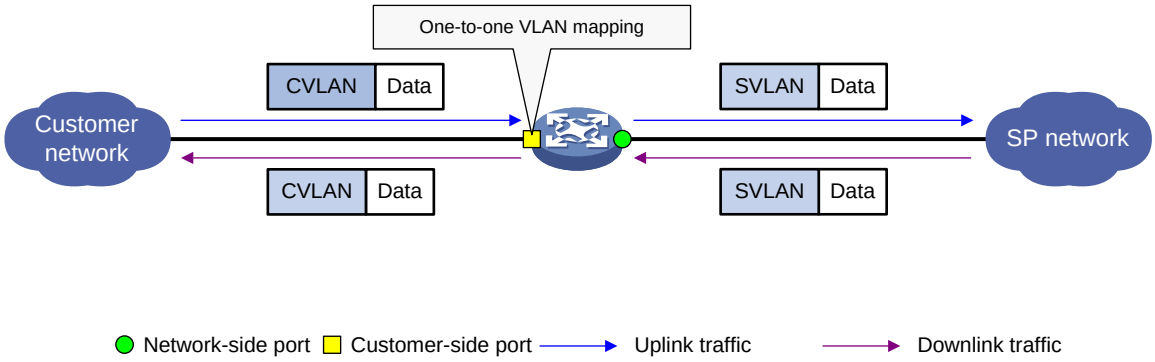


One-to-one VLAN mapping

As shown in Figure 66, one-to-one VLAN mapping is implemented on the customer-side port and replaces VLAN tags as follows:

- Replaces the CVLAN with the SVLAN for the uplink traffic.
- Replaces the SVLAN with the CVLAN for the downlink traffic.

Figure 66 One-to-one VLAN mapping implementation

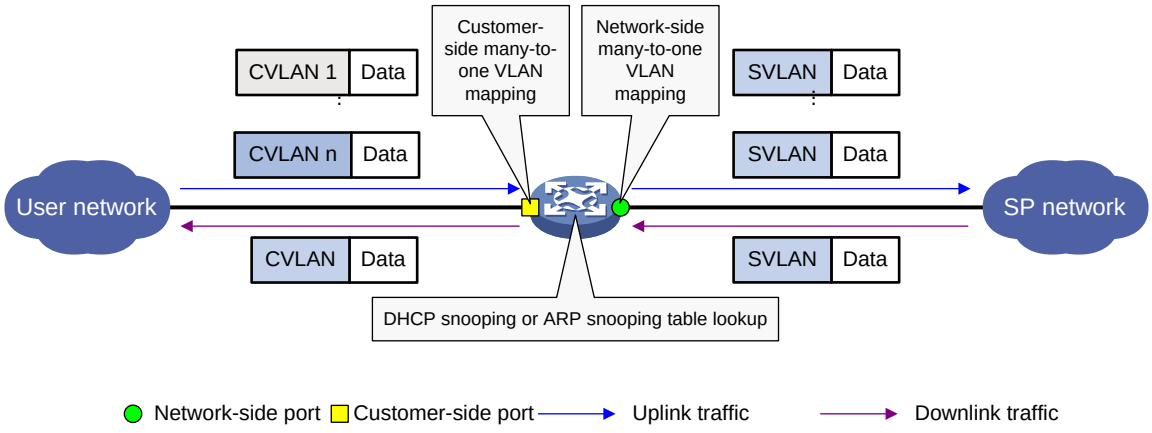


Many-to-one VLAN mapping

As shown in Figure 67, many-to-one VLAN mapping is implemented on both the customer-side and network-side ports as follows:

- For the uplink traffic, the customer-side many-to-one VLAN mapping replaces multiple CVLANs with the same SVLAN.
- For the downlink traffic, the network-side many-to-one VLAN mapping replaces the SVLAN with the CVLAN found in the DHCP snooping table or ARP snooping table. For more information about DHCP snooping or ARP snooping, see *Layer 3—IP Services Configuration Guide*.

Figure 67 Many-to-one VLAN mapping implementation



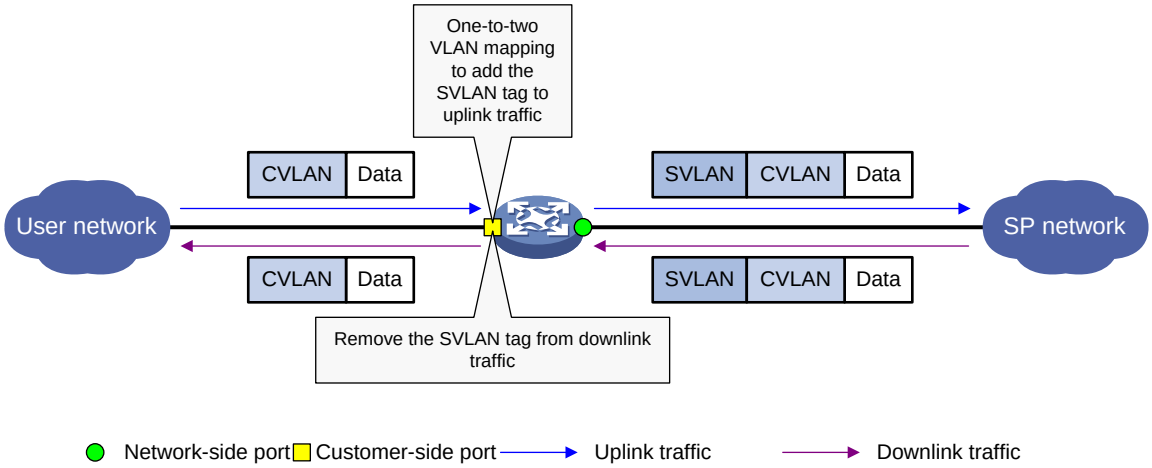
One-to-two VLAN mapping

As shown in Figure 68, one-to-two VLAN mapping is implemented on the customer-side port to add the SVLAN tag for the uplink traffic.

For the downlink traffic to be correctly sent to the customer network, make sure the SVLAN tag is removed on the customer-side port before transmission. Use one of the following methods to remove the SVLAN tag from the downlink traffic:

- Configure the customer-side port as a hybrid port and assign the port to the SVLAN as an untagged member.
- Configure the customer-side port as a trunk port and configure the SVLAN as the PVID.

Figure 68 One-to-two VLAN mapping implementation

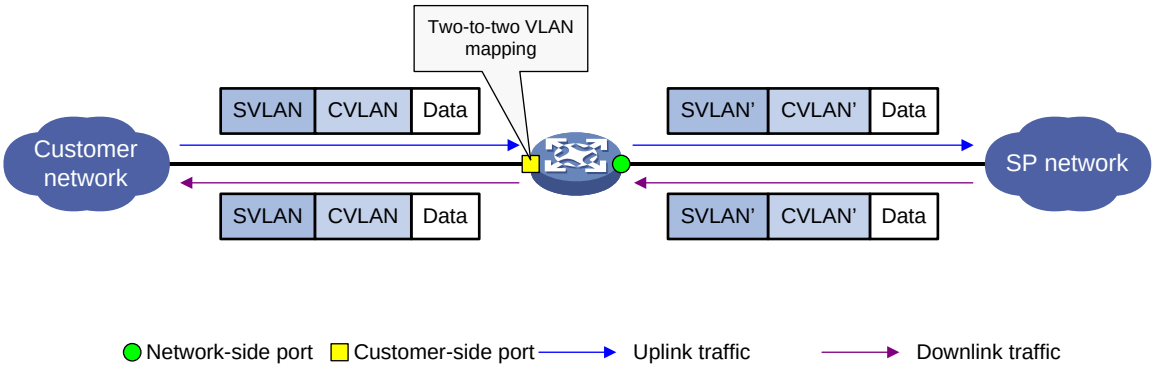


Two-to-two VLAN mapping

As shown in Figure 69, two-to-two VLAN mapping is implemented on the customer-side port and replaces VLAN tags as follows:

- Replaces the CVLAN and the SVLAN with the CVLAN' and the SVLAN' for the uplink traffic.
- Replaces the SVLAN' and CVLAN' with the SVLAN and the CVLAN for the downlink traffic.

Figure 69 Two-to-two VLAN mapping implementation



General configuration restrictions and guidelines

When you configure VLAN mapping, follow these restrictions and guidelines:

- When you configure one-to-two VLAN mapping on a QinQ-enabled port, the switch operates as follows:
  - If a packet matches the one-to-two VLAN mapping, the switch tags the packet with the SVLAN that is specified in the VLAN mapping.
  - If a packet does not match the one-to-two VLAN mapping, the switch tags the packet with the PVID.
- When you configure one-to-one or many-to-one VLAN mapping on a QinQ-enabled port, the switch operates as follows:
  - If a packet matches the one-to-one or many-to-one VLAN mapping, the switch replaces the CVLAN tag with the SVLAN tag specified in the VLAN mapping.
  - If a packet does not match the one-to-one or many-to-one VLAN mapping, the switch tags the packet with the PVID.

  For more information about QinQ, see "Configuring QinQ."
- You can configure both VLAN mapping and a QoS policy for VLAN tagging. The QoS policy takes effect if a configuration conflict occurs. For information about QoS policies, see *ACL and QoS Configuration Guide*.

VLAN mapping configuration task list

IMPORTANT:

Use the appropriate VLAN mapping methods for the devices in the network.

To configure VLAN mapping:

Tasks at a glance	Remarks
Configuring one-to-one VLAN mapping	Configure one-to-one VLAN mapping on the wiring-closet switch, as shown in Figure 63.
Configuring many-to-one VLAN mapping • Configuring many-to-one VLAN mapping in a network with dynamic IP address assignment • Configuring many-to-one VLAN mapping in a network with static IP address assignment	Configure many-to-one VLAN mapping on the campus switch, as shown in Figure 63. Complete one of the tasks based on the IP address assignment method.

Tasks at a glance	Remarks
• Configuring one-to-two VLAN mapping	Configure one-to-two VLAN mapping on PE 1 and PE 4, as shown in Figure 64, through which traffic from customer networks enter the service provider networks.
Configuring two-to-two VLAN mapping	Configure two-to-two VLAN mapping on PE 3, as shown in Figure 64, which is an edge device of the SP 2 network.

Configuring one-to-one VLAN mapping

Configure one-to-one VLAN mapping on the customer-side ports of wiring-closet switches (see Figure 63) to isolate traffic of the same service type from different homes.

Before you configure one-to-one VLAN mapping, create the original VLAN and the translated VLAN.

To configure one-to-one VLAN mapping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Set the link type of the port.	• Configure the port as a trunk port: **port link-type trunk** • Configure the port as a hybrid port: **port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the original VLANs and the translated VLANs.	• **port trunk permit vlan** *vlan-id-list* • **port hybrid vlan** *vlan-id-list* **tagged**	N/A
5. Configure a one-to-one VLAN mapping.	**vlan mapping** *vlan-id* **translated-vlan** *vlan-id*	By default, no VLAN mapping is configured on an interface.

Configuring many-to-one VLAN mapping

Configure many-to-one VLAN mapping on campus switches (see Figure 63) to transmit the same type of traffic from different users in one VLAN.

Configuring many-to-one VLAN mapping in a network with dynamic IP address assignment

In a network that uses dynamic address assignment, configure many-to-one VLAN mapping with DHCP snooping.

The switch replaces the SVLAN tag of the downlink traffic with the associated CVLAN tag based on the DHCP snooping entry lookup.

Configuration restrictions and guidelines

When you configure many-to-one VLAN mapping in a network that uses dynamic address assignment, follow these restrictions and guidelines:

- Before you configure many-to-one VLAN mapping, create the original VLANs and the translated VLANs.
- Customer-side many-to-one VLAN mapping is not supported on Layer 2 aggregate interfaces.
- To ensure correct traffic forwarding from the service provider network to the customer network, do not configure many-to-one VLAN mapping together with uRPF. For more information about uRPF, see *Security Configuration Guide*.
- To modify many-to-one VLAN mappings, first use the **reset dhcp snooping binding** command to clear the DHCP snooping entries.

Configuration task list

Tasks at a glance
(Required.) Enabling DHCP snooping
(Required.) Enabling ARP detection
(Required.) Configuring the customer-side port
(Required.) Configuring the network-side port

Enabling DHCP snooping

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable DHCP snooping.	**dhcp snooping enable**	By default, DHCP snooping is disabled. For more information about DHCP snooping configuration commands, see *Layer 3—IP Services Command Reference*.

Enabling ARP detection

Enable ARP detection for the original VLANs and the translated VLANs.

To enable ARP detection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Enable ARP detection.	**arp detection enable**	By default, ARP detection is disabled. For more information about ARP detection configuration commands, see

Step	Command	Remarks
		Security Command Reference.

Configuring the customer-side port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the link type of the port.	• Configure the port as a trunk port: **port link-type trunk** • Configure the port as a hybrid port: **port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the original VLANs and the translated VLANs.	• **port trunk permit vlan** *vlan-id-list* • **port hybrid vlan** *vlan-id-list* **tagged**	N/A
5. Configure a many-to-one VLAN mapping.	**vlan mapping uni** { **range** *vlan-range-list* | **single** *vlan-id-list* } **translated-vlan** *vlan-id*	By default, no VLAN mapping is configured on an interface.
6. Enable DHCP snooping entry recording.	**dhcp snooping binding record**	By default, DHCP snooping entry recording is disabled on an interface.

Configuring the network-side port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Set the link type of the port.	• Configure the port as a trunk port: **port link-type trunk** • Configure the port as a hybrid port: **port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the translated VLANs.	• **port trunk permit vlan** *vlan-id-list* • **port hybrid vlan** *vlan-id-list* **tagged**	N/A
5. Configure the port as a DHCP snooping trusted port.	**dhcp snooping trust**	By default, all ports that support DHCP snooping are untrusted ports when DHCP snooping is enabled.
6. Configure the port as an ARP	**arp detection trust**	By default, all ports are ARP

Step	Command	Remarks
trusted port.		untrusted ports.
7. Configure the port to use the original VLAN tags of the many-to-one mapping to replace the VLAN tags of the packets destined for the user network.	**vlan mapping nni**	By default, the port does not replace the VLAN tags of the packets destined for the user network.

Configuring many-to-one VLAN mapping in a network with static IP address assignment

In a network that uses static IP addresses, configure many-to-one VLAN mapping with ARP snooping.

The switch replaces the SVLAN tag of the downlink traffic with the associated CVLAN tag based on the ARP snooping entry lookup.

Configuration restrictions and guidelines

When you configure many-to-one VLAN mapping in a network that uses static address assignment, follow these restrictions and guidelines:

- Before you configure many-to-one VLAN mapping, create the original VLANs and the translated VLANs.
- Make sure two hosts in different CVLANs do not use the same IP address.
- When an IP address is no longer associated with the MAC address in a VLAN as in the ARP snooping table, perform one of the following operations:
  - Use the **reset arp snooping ip** *ip-address* command to clear this ARP snooping entry.
  - Wait for this ARP snooping entry to be aged out.
- Customer-side many-to-one VLAN mapping is not supported on Layer 2 aggregate interfaces.
- Before you modify many-to-one VLAN mappings, use the **reset arp snooping vlan** *vlan-id* command to clear the ARP snooping entries in each CVLAN.
- To ensure correct traffic forwarding from the service provider network to the customer network, do not configure many-to-one VLAN mapping together with uRPF. For more information about uRPF, see *Security Configuration Guide*.

Configuration task list

Tasks at a glance
(Required.) Enabling ARP snooping
(Required.) Configuring the customer-side port
(Required.) Configuring the network-side port

Enabling ARP snooping

Enable ARP snooping for the original VLANs and the translated VLANs.

To enable ARP snooping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Enable ARP snooping.	**arp snooping enable**	By default, ARP snooping is disabled. For more information about ARP snooping commands, see *Layer 3—IP Services Command Reference*.

Configuring the customer-side port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the link type of the port.	• Configure the port as a trunk port: **port link-type trunk** • Configure the port as a hybrid port: **port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the original VLANs and the translated VLANs.	• **port trunk permit vlan** *vlan-id-list* • **port hybrid vlan** *vlan-id-list* **tagged**	N/A
5. Configure a many-to-one VLAN mapping.	**vlan mapping uni** { **range** *vlan-range-list* | **single** *vlan-id-list* } **translated-vlan** *vlan-id*	By default, no VLAN mapping is configured on an interface.

Configuring the network-side port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Set the link type of the port.	• Configure the port as a trunk port: **port link-type trunk** • Configure the port as a hybrid port: **port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the translated VLANs.	• **port trunk permit vlan** *vlan-id-list* • **port hybrid vlan** *vlan-id-list* **tagged**	N/A
5. Configure the port to use the original VLAN tags of the many-to-one mapping to	**vlan mapping nni**	By default, the port does not replace the VLAN tags of the

Step	Command	Remarks
replace the VLAN tags of the packets destined for the user network.		packets destined for the user network.

Configuring one-to-two VLAN mapping

Configure one-to-two VLAN mapping on customer-side ports of the edge devices from which customer traffic enters SP networks, for example, on PE 1 and PE 4 in Figure 64. One-to-two VLAN mapping enables the edge devices to add an SVLAN tag to each incoming packet.

Before you configure one-to-two VLAN mapping, create the CVLAN and the SVLAN.

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet in the service provider network.

To configure one-to-two VLAN mapping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Configure the link type of the port as hybrid.	**port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the CVLANs.	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
5. Assign the port to the SVLANs as an untagged member.	**port hybrid vlan** *vlan-id-list* **untagged**	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
6. Configure a one-to-two VLAN mapping.	**vlan mapping nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id*	By default, no VLAN mapping is configured on an interface.

Configuring two-to-two VLAN mapping

Configure two-to-two VLAN mapping on the customer-side port of an edge device that connects two SP networks, for example, on PE 3 in Figure 64. Two-to-two VLAN mapping enables two sites in different VLANs to communicate at Layer 2 across two service provider networks that use different VLAN assignment schemes.

Before you configure two-to-two VLAN mapping, create the original VLANs and the translated VLANs.

To configure two-to-two VLAN mapping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Set the link type of the port.	• Configure the port as a trunk port: **port link-type trunk** • Configure the port as a hybrid port: **port link-type hybrid**	By default, the link type of a port is **access**.
4. Assign the port to the original VLANs and the translated VLANs.	• **port trunk permit vlan** *vlan-id-list* • **port hybrid vlan** *vlan-id-list* **tagged**	N/A
5. Configure a two-to-two VLAN mapping.	**vlan mapping tunnel** *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id*	By default, no VLAN mapping is configured on an interface.

Displaying and maintaining VLAN mapping

Execute **display** commands in any view.

Task	Command
Display VLAN mapping information.	**display vlan mapping** [**interface** *interface-type interface-number*]

VLAN mapping configuration examples

One-to-one and many-to-one VLAN mapping configuration example

Network requirements

As shown in Figure 70:

- Each household subscribes to PC, VoD, and VoIP services, and obtains the IP address through DHCP.
- On the home gateways, VLANs 1, 2, and 3 are assigned to PC, VoD, and VoIP traffic, respectively.

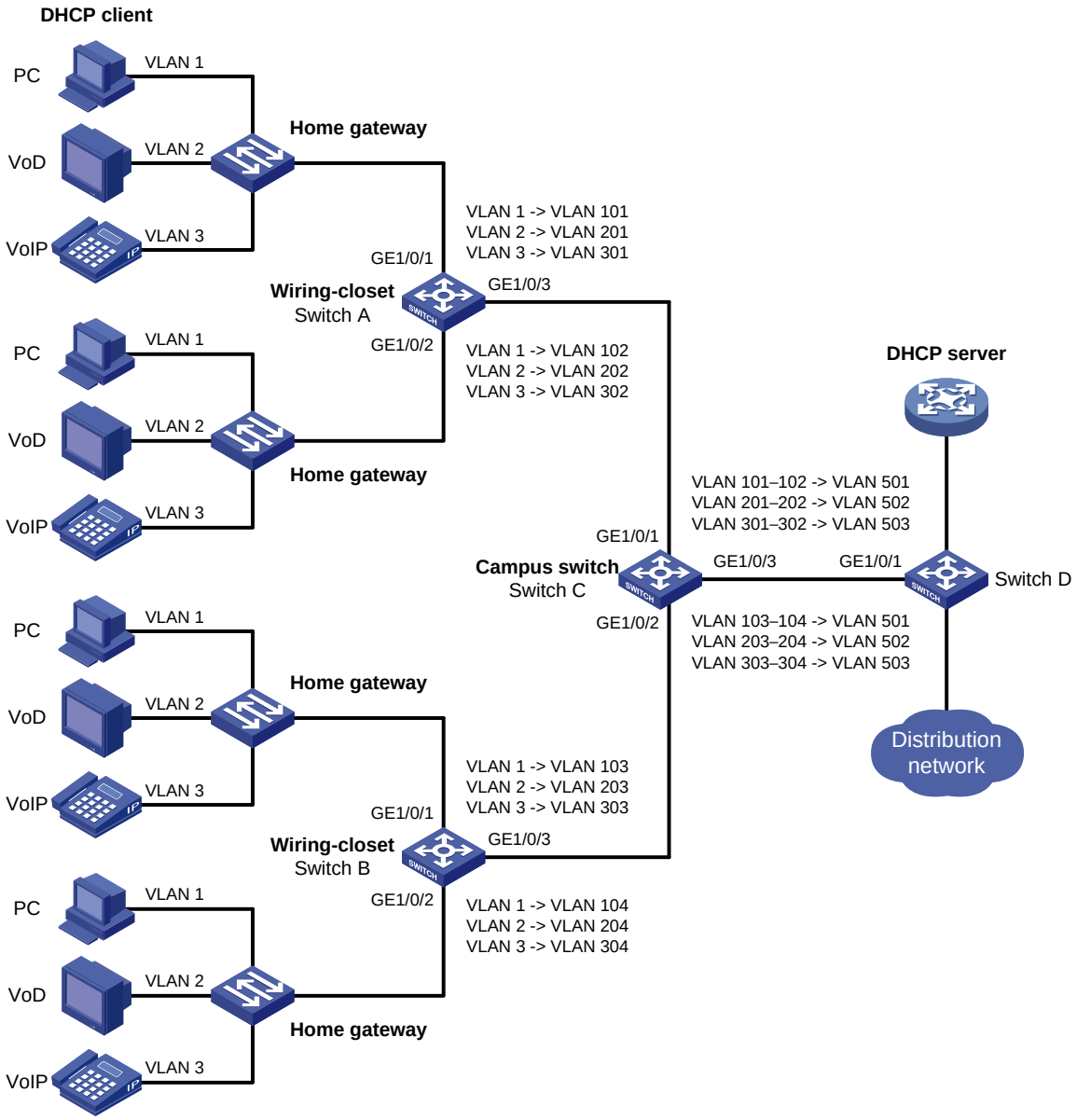
To isolate traffic of the same service type from different households, configure one-to-one VLAN mappings on the wiring-closet switches. This feature assigns one VLAN to each type of traffic from each household.

To save VLAN resources, configure many-to-one VLAN mappings on the campus switch (Switch C). This feature transmits the same type of traffic from different households in one VLAN. Use VLANs 501, 502, and 503 for PC, VoD, and VoIP traffic, respectively.

Table 17 VLAN mapping for each service

Service	VLANs on home gateways	VLANs on wiring-closet switches (Switch A and Switch B)	VLANs on campus switch (Switch C)
PC	VLAN 1	VLANs 101, 102, 103, 104	VLAN 501
VoD	VLAN 2	VLANs 201, 202, 203, 204	VLAN 502
VoIP	VLAN 3	VLANs 301, 302, 303, 304	VLAN 503

Figure 70 Network diagram



Configuration procedure

1. Configure Switch A:

Create the original VLANs.

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
```

Create the translated VLANs.

```
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

Configure the customer-side port GigabitEthernet 1/0/1 as a trunk port, and assign the port to all original VLANs and translated VLANs.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301
```

Configure one-to-one VLAN mappings on GigabitEthernet 1/0/1 to map VLANs 1, 2, and 3 to VLANs 101, 201, and 301, respectively.

```
[SwitchA-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
[SwitchA-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201
[SwitchA-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure the customer-side port GigabitEthernet 1/0/2 as a trunk port, and assign the port to all original VLANs and translated VLANs.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302
```

Configure one-to-one VLAN mappings on GigabitEthernet 1/0/2 to map VLANs 1, 2, and 3 to VLANs 102, 202, and 302, respectively.

```
[SwitchA-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102
[SwitchA-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202
[SwitchA-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure the network-side port GigabitEthernet 1/0/3 as a trunk port, and assign the port to the translated VLANs.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
[SwitchA-GigabitEthernet1/0/3] quit
```

2. Configure Switch B in the same way Switch A is configured. (Details not shown.)

3. Configure Switch C:

Enable DHCP snooping.

```
<SwitchC> system-view
[SwitchC] dhcp snooping enable
```

Create the original VLANs and translated VLANs, and enable ARP detection for these VLANs.

```
[SwitchC] vlan 101
[SwitchC-vlan101] arp detection enable
[SwitchC-vlan101] vlan 201
[SwitchC-vlan201] arp detection enable
[SwitchC-vlan201] vlan 301
[SwitchC-vlan301] arp detection enable
```

```
[SwitchC-vlan301] vlan 102
[SwitchC-vlan102] arp detection enable
[SwitchC-vlan102] vlan 202
[SwitchC-vlan202] arp detection enable
[SwitchC-vlan202] vlan 302
[SwitchC-vlan302] arp detection enable
[SwitchC-vlan302] vlan 103
[SwitchC-vlan103] arp detection enable
[SwitchC-vlan103] vlan 203
[SwitchC-vlan203] arp detection enable
[SwitchC-vlan203] vlan 303
[SwitchC-vlan303] arp detection enable
[SwitchC-vlan303] vlan 104
[SwitchC-vlan104] arp detection enable
[SwitchC-vlan104] vlan 204
[SwitchC-vlan204] arp detection enable
[SwitchC-vlan204] vlan 304
[SwitchC-vlan304] arp detection enable
[SwitchC-vlan304] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan501] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan502] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit
```

Configure the customer-side port GigabitEthernet 1/0/1 as a trunk port, and assign the port to original VLANs and translated VLANs.

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 101 102 201 202 301 302 501 to
503
```

Configure many-to-one VLAN mappings on the customer-side port GigabitEthernet 1/0/1 to map VLANs for PC, VoD, and VoIP traffic to VLANs 501, 502, and 503, respectively.

```
[SwitchC-GigabitEthernet1/0/1] vlan mapping uni range 101 to 102 translated-vlan 501
[SwitchC-GigabitEthernet1/0/1] vlan mapping uni range 201 to 202 translated-vlan 502
[SwitchC-GigabitEthernet1/0/1] vlan mapping uni range 301 to 302 translated-vlan 503
```

Enable DHCP snooping entry recording on GigabitEthernet 1/0/1.

```
[SwitchC-GigabitEthernet1/0/1] dhcp snooping binding record
[SwitchC-GigabitEthernet1/0/1] quit
```

Configure the customer-side port GigabitEthernet 1/0/2 as a trunk port, and assign the port to original VLANs and translated VLANs.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 103 104 203 204 303 304 501 to
503
```

Configure many-to-one VLAN mappings on the customer-side port GigabitEthernet 1/0/2 to map VLANs for PC, VoD, and VoIP traffic to VLANs 501, 502, and 503, respectively.

```
[SwitchC-GigabitEthernet1/0/2] vlan mapping uni range 103 to 104 translated-vlan 501
[SwitchC-GigabitEthernet1/0/2] vlan mapping uni range 203 to 204 translated-vlan 502
```

```
[SwitchC-GigabitEthernet1/0/2] vlan mapping uni range 303 to 304 translated-vlan 503
```

Enable DHCP snooping entry recording on GigabitEthernet 1/0/2.

```
[SwitchC-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchC-GigabitEthernet1/0/2] quit
```

Configure the network-side port GigabitEthernet 1/0/3 to use the original VLAN tags of the many-to-one mappings to replace the VLAN tags of the packets destined for the user network.

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] vlan mapping nni
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign the port to the translated VLANs.

```
[SwitchC-GigabitEthernet1/0/3] port link-type trunk
[SwitchC-GigabitEthernet1/0/3] port trunk permit vlan 501 to 503
```

Configure GigabitEthernet 1/0/3 as a DHCP snooping trusted and ARP trusted port.

```
[SwitchC-GigabitEthernet1/0/3] dhcp snooping trust
[SwitchC-GigabitEthernet1/0/3] arp detection trust
[SwitchC-GigabitEthernet1/0/3] quit
```

4. Configure Switch D:

Create the translated VLANs.

```
<SwitchD> system-view
[SwitchD] vlan 501 to 503
```

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to the translated VLANs 501 through 503.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 501 to 503
[SwitchD-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify VLAN mapping information on the wiring-closet switches, for example, Switch A.

```
[SwitchA] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           101                      N/A
  2             N/A           201                      N/A
  3             N/A           301                      N/A
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           102                      N/A
  2             N/A           202                      N/A
  3             N/A           302                      N/A
```

Verify VLAN mapping information on Switch C.

```
[SwitchC] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  101-102       N/A           501                      N/A
  201-202       N/A           502                      N/A
  301-302       N/A           503                      N/A
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
```

```
103-104        N/A            501                        N/A
203-204        N/A            502                        N/A
303-304        N/A            503                        N/A
```

One-to-two and two-to-two VLAN mapping configuration example

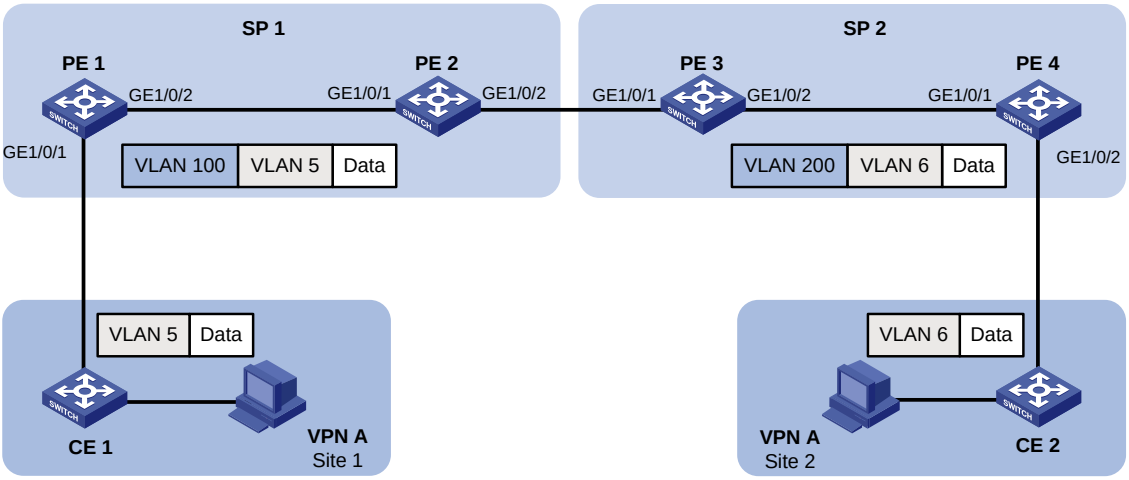
Network requirements

As shown in Figure 71:

- Two VPN A branches, Site 1 and Site 2, are in VLAN 5 and VLAN 6, respectively.
- The two sites use different VPN access services from different service providers, SP 1 and SP 2.
- SP 1 assigns VLAN 100 to Site 1 and Site 2. SP 2 assigns VLAN 200 to Site 1 and Site 2.

Configure one-to-two VLAN mappings and a two-to-two VLAN mapping to enable the two branches to communicate across networks SP 1 and SP 2.

Figure 71 Network diagram



Configuration procedure

1. Configure PE 1:

   # Configure a one-to-two VLAN mapping on the customer-side port GigabitEthernet 1/0/1 to add SVLAN tag 100 to traffic from VLAN 5.

   ```
   <PE1> system-view
   [PE1] interface gigabitethernet 1/0/1
   [PE1-GigabitEthernet1/0/1] vlan mapping nest single 5 nested-vlan 100
   ```

   # Configure GigabitEthernet 1/0/1 as a hybrid port. Assign the port to VLAN 5 and VLAN 100 as a tagged member and an untagged member, respectively.

   ```
   [PE1-GigabitEthernet1/0/1] port link-type hybrid
   [PE1-GigabitEthernet1/0/1] port hybrid vlan 5 tagged
   [PE1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
   [PE1-GigabitEthernet1/0/1] quit
   ```

   # Configure the network-side port GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLAN 100.

   ```
   [PE1] interface gigabitethernet 1/0/2
   [PE1-GigabitEthernet1/0/2] port link-type trunk
   ```

```
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE1-GigabitEthernet1/0/2] quit
```

2. Configure PE 2:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLAN 100.

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100
[PE2-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLAN 100.

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE2-GigabitEthernet1/0/2] quit
```

3. Configure PE 3:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLANs 100 and 200.

```
<PE3> system-view
[PE3] interface gigabitethernet 1/0/1
[PE3-GigabitEthernet1/0/1] port link-type trunk
[PE3-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

Configure a two-to-two VLAN mapping on GigabitEthernet 1/0/1 to map SVLAN 100 and CVLAN 5 to SVLAN 200 and CVLAN 6.

```
[PE3-GigabitEthernet1/0/1] vlan mapping tunnel 100 5 translated-vlan 200 6
[PE3-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLAN 200.

```
[PE3] interface gigabitethernet 1/0/2
[PE3-GigabitEthernet1/0/2] port link-type trunk
[PE3-GigabitEthernet1/0/2] port trunk permit vlan 200
[PE3-GigabitEthernet1/0/2] quit
```

4. Configure PE 4:

Configure the network-side port GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLAN 200.

```
<PE4> system-view
[PE4] interface gigabitethernet 1/0/1
[PE4-GigabitEthernet1/0/1] port link-type trunk
[PE4-GigabitEthernet1/0/1] port trunk permit vlan 200
[PE4-GigabitEthernet1/0/1] quit
```

Configure the customer-side port GigabitEthernet 1/0/2 as a hybrid port. Assign the port to VLAN 6 and VLAN 200 as a tagged member and an untagged member, respectively.

```
[PE4] interface gigabitethernet 1/0/2
[PE4-GigabitEthernet1/0/2] port link-type hybrid
[PE4-GigabitEthernet1/0/2] port hybrid vlan 6 tagged
[PE4-GigabitEthernet1/0/2] port hybrid vlan 200 untagged
```

Configure a one-to-two VLAN mapping on the customer-side port GigabitEthernet 1/0/2 to add SVLAN tag 200 to traffic from VLAN 6.

```
[PE4-GigabitEthernet1/0/2] vlan mapping nest single 6 nested-vlan 200
[PE4-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify VLAN mapping information on PE 1.

```
[PE1] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  5             N/A           100                      5
```

Verify VLAN mapping information on PE 3.

```
[PE3] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  100           5             200                      6
```

Verify VLAN mapping information on PE 4.

```
[PE4] display vlan mapping
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  6             N/A           200                      6
```

Configuring LLDP

You can set an Ethernet interface to work in Layer 3 mode by using the **port link-mode route** command (see "Configuring Ethernet interfaces").

Overview

In a heterogeneous network, a standard configuration exchange platform makes sure different types of network devices from different vendors can discover one another and exchange configuration.

The Link Layer Discovery Protocol (LLDP) is specified in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to the directly connected devices. Local device information includes its system capabilities, management IP address, device ID, and port ID. The device stores the device information in LLDPDUs from the LLDP neighbors in a standard MIB. For more information about MIBs, see *Network Management and Monitoring Configuration Guide*. LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

Basic concepts

LLDP agent

An LLDP agent is a mapping of an entity where LLDP runs. Multiple LLDP agents can run on the same interface.

LLDP agents are divided into the following types:

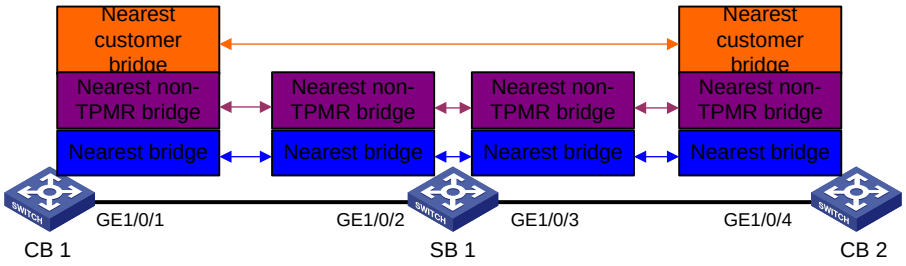
- Nearest bridge agent.
- Nearest customer bridge agent.
- Nearest non-TPMR bridge agent.

A Two-port MAC Relay (TPMR) is a type of bridge that has only two externally-accessible bridge ports, and supports a subset of the functions of a MAC bridge. A TPMR is transparent to all frame-based media-independent protocols except for the following:

- Protocols destined to it.
- Protocols destined to reserved MAC addresses that the relay function of the TPMR is configured not to forward.

LLDP exchanges packets between neighbor agents and creates and maintains neighbor information for them. Figure 72 shows the neighbor relationships for these LLDP agents. LLDP has two bridge modes: customer bridge (CB) and service bridge (SB).

Figure 72 LLDP neighbor relationships



LLDP frame formats

LLDP sends device information in LLDP frames. LLDP frames are encapsulated in Ethernet II or SNAP frames.

- LLDP frame encapsulated in Ethernet II

Figure 73 Ethernet II-encapsulated LLDP frame

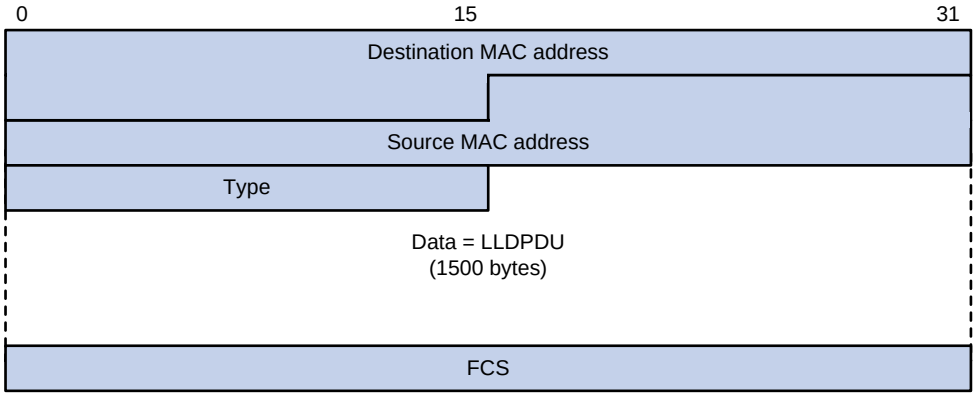


Table 18 Fields in an Ethernet II-encapsulated LLDP frame

Field	Description
Destination MAC address	MAC address to which the LLDP frame is advertised. LLDP specifies different multicast MAC addresses as destination MAC addresses for LLDP frames destined for agents of different types. This helps distinguish between LLDP frames sent and received by different agent types on the same interface. The destination MAC address is fixed to one of the following multicast MAC addresses: • 0x0180-C200-000E for LLDP frames destined for nearest bridge agents. • 0x0180-C200-0000 for LLDP frames destined for nearest customer bridge agents. • 0x0180-C200-0003 for LLDP frames destined for nearest non-TPMR bridge agents.
Source MAC address	MAC address of the sending port.
Type	Ethernet type for the upper-layer protocol. It is 0x88CC for LLDP.
Data	LLDPDU. An LLDP frame contains only one LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

- LLDP frame encapsulated in SNAP

Figure 74 SNAP-encapsulated LLDP frame

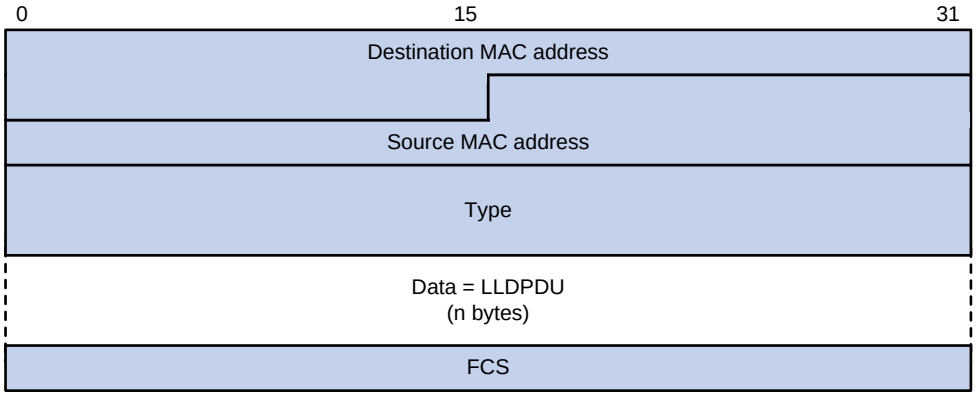


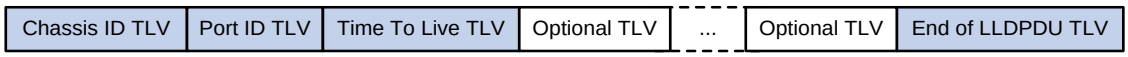
Table 19 Fields in a SNAP-encapsulated LLDP frame

Field	Description
Destination MAC address	MAC address to which the LLDP frame is advertised. It is the same as that for Ethernet II-encapsulated LLDP frames.
Source MAC address	MAC address of the sending port.
Type	SNAP type for the upper-layer protocol. It is 0xAAAA-0300-0000-88CC for LLDP.
Data	LLDPDU. An LLDP frame contains only one LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

LLDPDUs

LLDP uses LLDPDUs to exchange information. An LLDPDU comprises multiple TLVs. Each TLV carries a type of device information, as shown in Figure 75.

Figure 75 LLDPDU encapsulation format



An LLDPDU can carry up to 32 types of TLVs. Mandatory TLVs include Chassis ID TLV, Port ID TLV, Time to Live TLV, and End of LLDPDU TLV. Other TLVs are optional.

TLVs

A TLV is an information element that contains the type, length, and value fields.

LLDPDU TLVs include the following categories:

- Basic management TLVs
- Organizationally (IEEE 802.1 and IEEE 802.3) specific TLVs
- LLDP-MED (media endpoint discovery) TLVs

Basic management TLVs are essential to device management.

Organizationally specific TLVs and LLDP-MED TLVs are used for enhanced device management. They are defined by standardization or other organizations and are optional for LLDPDUs.

- Basic management TLVs

  Table 20 lists the basic management TLV types. Some of them are mandatory for LLDPDUs.

Table 20 Basic management TLVs

Type	Description	Remarks
Chassis ID	Specifies the bridge MAC address of the sending device.	Mandatory.
Port ID	Specifies the ID of the sending port: • If the LLDPDU carries LLDP-MED TLVs, the port ID TLV carries the MAC address of the sending port. • Otherwise, the port ID TLV carries the port name.	
Time to Live	Specifies the life of the transmitted information on the receiving device.	
End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU.	
Port Description	Specifies the description for the sending port.	Optional.
System Name	Specifies the assigned name of the sending device.	
System Description	Specifies the description for the sending device.	
System Capabilities	Identifies the primary functions of the sending device and the enabled primary functions.	
Management Address	Specifies the following elements: • The management address of the local device. • The interface number and object identifier (OID) associated with the address.	

- IEEE 802.1 organizationally specific TLVs

Table 21 IEEE 802.1 organizationally specific TLVs

Type	Description
Port VLAN ID	Specifies the port VLAN identifier (PVID).
Port And Protocol VLAN ID	Indicates whether the device supports protocol VLANs and, if so, what VLAN IDs these protocols will be associated with.
VLAN Name	Specifies the textual name of any VLAN to which the port belongs.
Protocol Identity	Indicates protocols supported on the port.
DCBX	Data center bridging exchange protocol. **NOTE:** The switch does not support DCBX TLV.
EVB module	Edge Virtual Bridging module, including EVB TLV and CDCP TLV. **NOTE:** The switch does not support EVB TLV.
Link Aggregation	Indicates whether the port supports link aggregation, and if yes, whether link aggregation is enabled.
Management VID	Management VLAN ID.
VID Usage Digest	VLAN ID usage digest.
ETS Configuration	Enhanced Transmission Selection configuration.
ETS Recommendation	ETS recommendation.
PFC	Priority-based Flow Control.
APP	Application protocol.

NOTE:

- HPE devices support only receiving protocol identity TLVs and VID usage digest TLVs.
- Layer 3 Ethernet ports support only link aggregation TLVs.

- IEEE 802.3 organizationally specific TLVs

  Table 22 IEEE 802.3 organizationally specific TLVs

Type	Description
MAC/PHY Configuration/Status	Contains the bit-rate and duplex capabilities of the sending port, support for autonegotiation, enabling status of autonegotiation, and the current rate and duplex mode.
Power Via MDI	Contains the power supply capabilities of the port: • Port class (PSE or PD). • Power supply mode. • Whether PSE power supply is supported. • Whether PSE power supply is enabled. • Whether pair selection can be controlled. • Power supply type. • Power source. • Power priority. • PD requested power. • PSE allocated power.
Maximum Frame Size	Indicates the supported maximum frame size. It is now the MTU of the port.
Power Stateful Control	Indicates the power state control configured on the sending port, including the following: • Power supply mode of the PSE/PD. • PSE/PD priority. • PSE/PD power.

NOTE:

The Power Stateful Control TLV is defined in IEEE P802.3at D1.0 and is not supported in later versions. HPE devices send this type of TLVs only after receiving them.

- LLDP-MED TLVs

  LLDP-MED TLVs provide multiple advanced applications for voice over IP (VoIP), such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs provide a cost-effective and easy-to-use solution for deploying voice devices in Ethernet. LLDP-MED TLVs are shown in Table 23.

  Table 23 LLDP-MED TLVs

Type	Description
LLDP-MED Capabilities	Allows a network device to advertise the LLDP-MED TLVs that it supports.
Network Policy	Allows a network device or terminal device to advertise the VLAN ID of a port, the VLAN type, and the Layer 2 and Layer 3 priorities for specific applications.
Extended Power-via-MDI	Allows a network device or terminal device to advertise power supply capability. This TLV is an extension of the Power Via MDI TLV.

Type	Description
Hardware Revision	Allows a terminal device to advertise its hardware version.
Firmware Revision	Allows a terminal device to advertise its firmware version.
Software Revision	Allows a terminal device to advertise its software version.
Serial Number	Allows a terminal device to advertise its serial number.
Manufacturer Name	Allows a terminal device to advertise its vendor name.
Model Name	Allows a terminal device to advertise its model name.
Asset ID	Allows a terminal device to advertise its asset ID. The typical case is that the user specifies the asset ID for the endpoint to facilitate directory management and asset tracking.
Location Identification	Allows a network device to advertise the appropriate location identifier information for a terminal device to use in the context of location-based applications.

NOTE:

- If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised even if they are advertisable.
- If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised even if they are advertisable.

Management address

The network management system uses the management address of a device to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

Working mechanism

LLDP operating modes

An LLDP agent can operate in one of the following modes:

- **TxRx mode**—An LLDP agent in this mode can send and receive LLDP frames.
- **Tx mode**—An LLDP agent in this mode can only send LLDP frames.
- **Rx mode**—An LLDP agent in this mode can only receive LLDP frames.
- **Disable mode**—An LLDP agent in this mode cannot send or receive LLDP frames.

Each time the LLDP operating mode of an LLDP agent changes, its LLDP protocol state machine reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, an LLDP agent must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.

Transmitting LLDP frames

An LLDP agent operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes. To prevent LLDP frames from overwhelming the network during times of frequent changes to local device information, LLDP uses the token bucket mechanism to rate limit LLDP frames. For more information about the token bucket mechanism, see *ACL and QoS Configuration Guide*.

LLDP automatically enables the fast LLDP frame transmission mechanism in either of the following cases:

- A new neighbor is discovered. A new LLDP frame is received and carries device information new to the local device.

- The LLDP operating mode of the LLDP agent changes from Disable or Rx to TxRx or Tx.

With this mechanism, the specified number of LLDP frames are sent successively at a configurable fast transmission interval to help LLDP neighbors discover the local device as soon as possible. Then, the normal LLDP frame transmission interval resumes.

Receiving LLDP frames

An LLDP agent operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the LLDP agent saves the information and starts an aging timer. When the TTL value in the Time To Live TLV carried in the LLDP frame becomes zero, the information ages out immediately.

Protocols and standards

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- IEEE 802.1AB-2009, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*
- *DCB Capability Exchange Protocol Specification Rev 1.00*
- *DCB Capability Exchange Protocol Base Specification Rev 1.01*
- IEEE Std 802.1Qaz-2011, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes*

LLDP configuration task list

Tasks at a glance
Performing basic LLDP configurations: • (Required.) Enabling LLDP • (Optional.) Configuring the LLDP bridge mode • (Optional.) Setting the LLDP operating mode • (Optional.) Setting the LLDP reinitialization delay • (Optional.) Enabling LLDP polling • (Optional.) Configuring the advertisable TLVs • (Optional.) Configuring the management address and its encoding format • (Optional.) Setting other LLDP parameters • (Optional.) Setting an encapsulation format for LLDP frames
(Optional.) Configuring CDP compatibility
(Optional.) Configuring LLDP trapping and LLDP-MED trapping

Performing basic LLDP configurations

Enabling LLDP

To make LLDP take effect on specific ports, you must enable LLDP both globally and on these ports.

To use LLDP together with OpenFlow, you must enable LLDP globally on OpenFlow switches. As a best practice to prevent LLDP from affecting topology discovery of OpenFlow controllers, disable LLDP on ports of OpenFlow instances. For more information about OpenFlow, see *OpenFlow Configuration Guide*.

To enable LLDP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable LLDP globally.	**lldp global enable**	By default: • If the switch starts up with empty configuration, LLDP is disabled globally (initial setting). • If the switch starts up with the default configuration file, LLDP is enabled globally (factory default). For more information about empty configuration and the default configuration file, see *Fundamentals Configuration Guide*.
3. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
4. Enable LLDP.	**lldp enable**	By default, LLDP is enabled on a port.

Configuring the LLDP bridge mode

The following LLDP bridge modes are available:

- **Customer bridge mode**—In customer bridge mode, LLDP supports nearest bridge agents, nearest non-TPMR bridge agents, and nearest customer bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in VLANs.
- **Service bridge mode**—In service bridge mode, LLDP supports nearest bridge agents and nearest non-TPMR bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in VLANs.

To configure the LLDP bridge mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure LLDP to operate in service bridge mode.	**lldp mode service-bridge**	By default, LLDP operates in customer bridge mode.

Setting the LLDP operating mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Set the LLDP operating mode.	• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view: **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** } • In Layer 2/Layer 3 aggregate interface view: **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **admin-status** { **disable** | **rx** | **tx** | **txrx** }	By default: • The nearest bridge agent operates in **txrx** mode. • The nearest customer bridge agent and nearest non-TPMR bridge agent operate in **disable** mode. In Ethernet interface view, if no agent type is specified, the command configures the operating mode for nearest bridge agents. In aggregate interface view, you can configure the operating mode only for nearest customer bridge agents and nearest non-TPMR bridge agents.

Setting the LLDP reinitialization delay

When the LLDP operating mode changes on a port, the port initializes the protocol state machines after an LLDP reinitialization delay. By adjusting the delay, you can avoid frequent initializations caused by frequent changes to the LLDP operating mode on a port.

To set the LLDP reinitialization delay for ports:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the LLDP reinitialization delay.	**lldp timer reinit-delay** *delay*	The default setting is 2 seconds.

Enabling LLDP polling

With LLDP polling enabled, a device periodically searches for local configuration changes. When the device detects a configuration change, it sends LLDP frames to inform neighboring devices of the change.

To enable LLDP polling:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable LLDP polling and set the polling interval.	• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view: **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval* • In Layer 2/Layer 3 aggregate interface view: **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*	By default, LLDP polling is disabled.

Configuring the advertisable TLVs

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the advertisable TLVs (in Layer 2 Ethernet interface view).	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] || **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } • **lldp agent nearest-nontpmr tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } }	By default: • Nearest bridge agents can advertise all types of LLDP TLVs except the DCBX TLV, location identification TLV, port and protocol VLAN ID TLVs, VLAN name TLVs, and management VLAN ID TLVs. • Nearest non-TPMR bridge agents advertise no TLVs. • Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs.

Step	Command	Remarks
	• **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } }	
4. Configure the advertisable TLVs (in Layer 3 Ethernet interface view or management Ethernet interface view).	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } • **lldp agent** { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }	By default: • Nearest bridge agents can advertise all types of LLDP TLVs (only link aggregation TLV in 802.1 organizationally specific TLVs) except network policy TLVs. • Nearest non-TPMR bridge agents advertise no TLVs. • Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV).
5. Configure the advertisable TLVs (in Layer 2 aggregate interface view).	• **lldp agent nearest-nontpmr tlv-enable** { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } } • **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } } • **lldp tlv-enable dot1-tlv** { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }	By default: • Nearest non-TPMR bridge agents advertise no TLVs. • Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only port and protocol VLAN ID TLV, VLAN name TLV, and management VLAN ID TLV). Nearest bridge agents are not supported on Layer 2 aggregate interfaces.
6. Configure the advertisable TLVs (in Layer 3 aggregate interface view).	**lldp agent** { **nearest-nontpmr** | **nearest-customer** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }	By default: • Nearest non-TPMR bridge agents advertise no TLVs. • Nearest customer bridge agents can advertise only basic TLVs.

Step	Command	Remarks
		Nearest bridge agents are not supported on Layer 3 aggregate interfaces.

A PoE-capable device of the series can act as a PSE. It supports autonegotiating the supplied power with the PD through LLDP. To use the function, you must perform the following tasks:

- Enable PoE and LLDP on the device.
- Enable PoE and LLDP on the port of the device connected to the PD.
- Configure the power field in IEEE 802.3 organizationally specific TLVs to enable the port to send power via MDI TLVs.

For more information about PoE, see *Network Management and Monitoring Configuration Guide*.

Configuring the management address and its encoding format

LLDP encodes management addresses in numeric or string format in management address TLVs.

By default, management addresses are encoded in numeric format. If a neighbor encodes its management address in string format, configure the encoding format of the management address as **string** on the connecting port. This guarantees normal communication with the neighbor.

To configure a management address to be advertised and its encoding format on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Allow LLDP to advertise the management address in LLDP frames and configure the advertised management address.	• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view: **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-enable basic-tlv management-address-tlv** [*ip-address*] • In Layer 2/Layer 3 aggregate interface view: **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv management-address-tlv** [*ip-address*]	By default: • Nearest bridge agents and nearest customer bridge agents can advertise the management address in LLDP frames. • Nearest non-TPMR bridge agents cannot advertise the management address in LLDP frames.
4. Configure the encoding format of the management address as string.	• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:	By default, the encoding format of the management address is numeric.

Step	Command	Remarks
	lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format string** • In Layer 2/Layer 3 aggregate interface view: **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **management-address-format string**	

Setting other LLDP parameters

The Time to Live TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can configure the TTL of locally sent LLDPDUs, which determines how long information about the local device can be saved on a neighboring device. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds. TTLs greater than 65535 will be rounded down to 65535 seconds.

To change LLDP parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the TTL multiplier.	**lldp hold-multiplier** *value*	The default setting is 4.
3. Set the LLDP frame transmission interval.	**lldp timer tx-interval** *interval*	The default setting is 30 seconds.
4. Set the token bucket size for sending LLDP frames.	**lldp max-credit** *credit-value*	The default setting is 5.
5. Set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.	**lldp fast-count** *count*	The default setting is 4.
6. Set the interval for fast LLDP frame transmission.	**lldp timer fast-interval** *interval*	The default setting is 1 second.

Setting an encapsulation format for LLDP frames

LLDP frames can be encapsulated in the following formats:

- **Ethernet II**—With Ethernet II encapsulation configured, an LLDP port sends LLDP frames in Ethernet II frames.
- **SNAP**—With SNAP encapsulation configured, an LLDP port sends LLDP frames in SNAP frames.

LLDP of earlier versions requires the same encapsulation format on both ends to process LLDP frames. To successfully communicate with a neighboring device running LLDP of earlier versions, the local device must be configured with the same encapsulation format.

To set the encapsulation format for LLDP frames to SNAP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Set the encapsulation format for LLDP frames to SNAP.	• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view: **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap** • In Layer 2/Layer 3 aggregate interface view: **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**	By default, Ethernet II encapsulation format applies.

Configuring CDP compatibility

When the switch is directly connected to a Cisco device that supports only CDP rather than LLDP, you can enable CDP compatibility to enable the switch to exchange information with the directly-connected device.

CDP compatibility enables the switch to use LLDP to receive and recognize CDP packets from the directly-connected device and send CDP packets to the directly-connected device. The packets that the switch sends to the neighboring CDP device carry the following information:

- Device ID.
- ID of the port connecting to the neighboring device.
- port IP address.
- PVID.
- TTL.

The port IP address is the primary IP address of the VLAN interface in up state. The VLAN ID of the VLAN interface must be the lowest among the VLANs permitted on the port. If no VLAN interfaces of the permitted VLANs is assigned an IP address or all VLAN interfaces are down, no port IP address will be advertised.

The CDP neighbor-information-related fields in the output of the **display lldp neighbor-information** command show the CDP neighboring device information that can be recognized by the switch. For more information about the **display lldp neighbor-information** command, see *Layer 2—LAN Switching Command Reference*.

If your LLDP-enabled device cannot recognize CDP packets, it does not respond to the requests of Cisco IP phones for the voice VLAN ID configured on the device. As a result, a requesting Cisco IP phone sends voice traffic without any VLAN tag to your device. Your device cannot differentiate the voice traffic from other types of traffic.

CDP compatibility enables your device to receive and recognize CDP packets from a Cisco IP phone and respond with CDP packets carrying TLVs with the voice VLAN configuration. According to TLVs with the voice VLAN configuration, the IP phone automatically configures the voice VLAN. As a result, the voice traffic is confined in the configured voice VLAN and is differentiated from other types of traffic.

For more information about voice VLANs, see "Configuring voice VLANs."

When the device is connected to a Cisco IP phone that has a host attached to its data port, the host must access the network through the Cisco IP phone. If the data port goes down, the IP phone will send a CDP packet to the device so the device can log out the user.

Configuration prerequisites

Before you configure CDP compatibility, complete the following tasks:

- Globally enable LLDP.
- Enable LLDP on the port connecting to a device supporting CDP.
- Configure LLDP to operate in TxRx mode on the port.

Configuration procedure

CDP-compatible LLDP operates in one of the following modes:

- **TxRx**—CDP packets can be transmitted and received.
- **Disable**—CDP packets cannot be transmitted or received.

To make CDP-compatible LLDP take effect on ports, follow these steps:

1. Enable CDP-compatible LLDP globally.
2. Configure CDP-compatible LLDP to operate in TxRx mode.

The maximum TTL value that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, configure the LLDP frame transmission interval to be no more than 1/3 of the TTL value.

To enable LLDP to be compatible with CDP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable CDP compatibility globally.	**lldp compliance cdp**	By default, CDP compatibility is disabled globally.
3. Enter Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Configure CDP-compatible LLDP to operate in TxRx mode.	**lldp compliance admin-status cdp txrx**	By default, CDP-compatible LLDP operates in **disable** mode.

Configuring LLDP trapping and LLDP-MED trapping

LLDP trapping or LLDP-MED trapping notifies the network management system of events such as newly detected neighboring devices and link failures.

To prevent excessive LLDP traps from being sent when the topology is unstable, set a trap transmission interval for LLDP.

To configure LLDP trapping and LLDP-MED trapping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable LLDP trapping.	• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view: **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable** • In Layer 2/Layer 3 aggregate interface view: **lldp agent** { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**	By default, LLDP trapping is disabled.
4. Enable LLDP-MED trapping (in Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view).	**lldp notification med-topology-change enable**	By default, LLDP-MED trapping is disabled.
5. Return to system view.	**quit**	N/A
6. (Optional.) Set the LLDP trap transmission interval.	**lldp timer notification-interval** *interval*	The default setting is 30 seconds.

Displaying and maintaining LLDP

Execute **display** commands in any view.

Task	Command
Display local LLDP information.	**display lldp local-information** [**global** | **interface** *interface-type interface-number*]
Display the information contained in the LLDP TLVs sent from neighboring devices.	**display lldp neighbor-information** [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]
Display LLDP statistics.	**display lldp statistics** [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]
Display LLDP status of a port.	**display lldp status** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]
Display types of advertisable optional LLDP TLVs.	**display lldp tlv-config** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

LLDP configuration examples

Basic LLDP configuration example

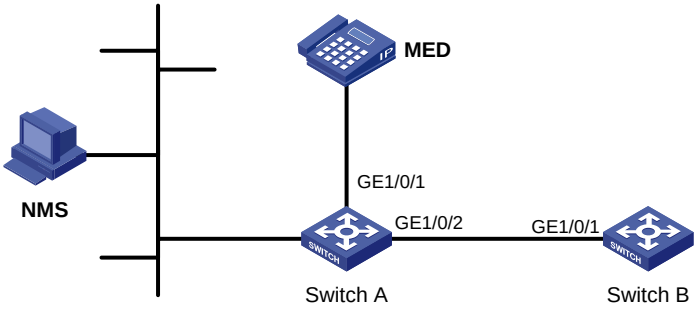
Network requirements

As shown in Figure 76, the NMS and Switch A are located in the same Ethernet network. A MED device and Switch B are connected to GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A.

Enable LLDP globally on Switch A and Switch B to perform the following tasks:

- Monitor the link between Switch A and Switch B.
- Monitor the link between Switch A and the MED device on the NMS.

Figure 76 Network diagram



Configuration procedure

1. Configure Switch A:

   # Enable LLDP globally.

   ```
   <SwitchA> system-view
   [SwitchA] lldp global enable
   ```

   # Enable LLDP on GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

   ```
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] lldp enable
   ```

   # Set the LLDP operating mode to Rx.

   ```
   [SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
   [SwitchA-GigabitEthernet1/0/1] quit
   ```

   # Enable LLDP on GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.

   ```
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] lldp enable
   ```

   # Set the LLDP operating mode to Rx.

   ```
   [SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
   [SwitchA-GigabitEthernet1/0/2] quit
   ```

2. Configure Switch B:

   # Enable LLDP globally.

   ```
   <SwitchB> system-view
   [SwitchB] lldp global enable
   ```

   # Enable LLDP on GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

   ```
   [SwitchB] interface gigabitethernet 1/0/1
   [SwitchB-GigabitEthernet1/0/1] lldp enable
   ```

Set the LLDP operating mode to Tx.

```
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
[SwitchB-GigabitEthernet1/0/1] quit
```

Verify the configuration:

Verify that:

- GigabitEthernet 1/0/1 of Switch A connects to a MED device.
- GigabitEthernet 1/0/2 of Switch A connects to a non-MED device.
- Both ports operate in Rx mode, and they can receive LLDP frames but cannot send LLDP frames.

```
[SwitchA] display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 2
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

```
LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 3

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

Remove the link between Switch A and Switch B.

Verify that GigabitEthernet 1/0/2 of Switch A does not connect to any neighboring devices.

```
[SwitchA] display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
```

```
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : RX_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
```

```
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

CDP-compatible LLDP configuration example

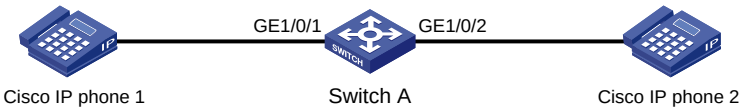
Network requirements

As shown in Figure 77, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone, which sends VLAN-tagged voice traffic.

Configure voice VLAN 2 on Switch A. Enable CDP compatibility of LLDP on Switch A to allow the Cisco IP phones to automatically configure the voice VLAN. The voice VLAN feature performs the following actions:

- Confines the voice traffic to the voice VLAN.
- Isolates the voice traffic from other types of traffic.

Figure 77 Network diagram



Configuration procedure

1. Configure a voice VLAN on Switch A:

   # Create VLAN 2.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] quit
   ```

   # Set the link type of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to trunk, and enable voice VLAN on them.

   ```
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-type trunk
   [SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
   [SwitchA-GigabitEthernet1/0/1] quit
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] port link-type trunk
   [SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
   ```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

2. Configure CDP-compatible LLDP on Switch A:

   # Enable LLDP globally, and enable CDP compatibility globally.

```
[SwitchA] lldp global enable
[SwitchA] lldp compliance cdp
```

   # Enable LLDP on GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

   # Configure LLDP to operate in TxRx mode on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx
```

   # Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit
```

   # Enable LLDP on GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

   # Configure LLDP to operate in TxRx mode on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx
```

   # Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that Switch A has completed the following tasks:

- Discovering the IP phones connected to GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
- Obtaining IP phone information.

```
[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
 CDP neighbor index  : 1
 Chassis ID          : SEP00141CBCDBFE
 Port ID             : Port 1
 Software version    : P0030301MFG2
 Platform            : Cisco IP Phone 7960
 Duplex              : Full

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
 CDP neighbor index  : 2
 Chassis ID          : SEP00141CBCDBFF
 Port ID             : Port 1
 Software version    : P0030301MFG2
 Platform            : Cisco IP Phone 7960
 Duplex              : Full
```

Configuring service loopback groups

A service loopback group contains one or multiple Ethernet ports for looping packets sent out by the device back to the device. This feature must work with other features, such as GRE.

A service loopback group provides one of the following services:

- **Tunnel**—Supports unicast tunnel traffic.
- **Multicast tunnel**—Supports multicast tunnel traffic.
- **Multiport**—Supports multiport ARP traffic.

The device supports only one service loopback group for each service type. You can use a service loopback group with multiple features.

Member ports in a service loopback group are load balanced.

Configuration procedure

Follow these guidelines when you configure a service loopback group:

- Make sure the ports you are assigning to a service loopback group meet the following requirements:
  - The ports are not used for any other purposes. The configuration on a port is removed when it is assigned to a service loopback group.
  - The ports support the service type of the service loopback group and are not members of any other service loopback group.
- You cannot change the service type of a service loopback group.
- For correct traffic processing, follow these guidelines:
  - Make sure the service loopback group has a minimum of one member port when it is being used by a feature.
  - Do not delete the service loopback group when it is being used by a feature.

To configure a service loopback group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a service loopback group and specify its service type.	**service-loopback group** *number* **type** { {**multicast-tunnel** | **tunnel** } *| **multiport** }	N/A
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Assign a port to the service loopback group.	**port service-loopback group** *number*	By default, a service loopback group does not contain ports. You can assign a maximum of 8 ports to a service loopback group.

Displaying and maintaining service loopback groups

Execute **display** commands in any view.

Task	Command
Display information about service loopback groups.	**display service-loopback group** [*number*]

Service loopback group configuration example

Network requirements

All Ethernet ports on Device A support the tunnel service.

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to a service loopback group to loop GRE packets sent out by the device back to the device.

Configuration procedure

Create service loopback group 1, and specify its service type as **tunnel**.

```
<DeviceA> system-view
[DeviceA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to service loopback group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Create the interface Tunnel 1 and set it to GRE mode. The interface will automatically use service loopback group 1.

```
[DeviceA] interface tunnel 1 mode gre
[DeviceA-Tunnel1]
```

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

Numerics

1:1 VLAN mapping
- application scenario, 214
- configuration, 220, 226
- implementation, 216, 217

1:2 VLAN mapping
- application scenario, 216
- configuration, 225, 231
- implementation, 216, 218

10-GE interface;010-GE interface
- combine, 2

2:2 VLAN mapping
- application scenario, 216
- configuration, 225, 231
- implementation, 216, 218

40-GE interface;040-GE interface
- split, 2

802
- 802.1 LLDPDU TLV types, 236
- 802.1Q-in-802.1Q. *Use* QinQ
- 802.3 LLDPDU TLV types, 236
- QinQ SVLAN tag 802.1p priority, 208
- VLAN group configuration, 141

A

accessing
- port-based VLAN assignment (access port), 132

action
- loop detection block, 122
- loop detection no-learning protection, 122
- loop detection protection action (Layer 2 aggregate interface), 124
- loop detection protection action configuration, 124
- loop detection shutdown protection, 122

adding
- MAC address table blackhole entry, 23
- MAC address table entry (global), 22
- MAC address table entry (on interface), 22
- MAC address table multiport unicast entry, 23

address
- MAC address learning disable, 24
- MAC Information queue length, 35

advertising
- LLDP advertisable TLV, 243
- voice VLAN advertisement (CDP), 181
- voice VLAN advertisement (LLDP), 181
- voice VLAN information advertisement to IP phones, 174

aggregating
- link. *See* link aggregation

aging
- MAC address table timer, 25
- spanning tree max age timer, 93

algorithm
- STP calculation, 74

alternate port (MST), 84

ARP
- MAC address table ARP fast update, 30

ARP detection
- M:1 VLAN mapping (dynamic IP address assignment), 221

ARP snooping
- M:1 VLAN mapping (static IP address assignment), 223

assigning
- MAC address table learning priority, 27
- MAC-based VLAN assignment (dynamic), 135
- MAC-based VLAN assignment (server-assigned), 136
- MAC-based VLAN assignment (static), 134
- port isolation group (multiple ports), 70
- port-based VLAN access port (interface view), 132
- port-based VLAN access port (VLAN view), 132
- port-based VLAN hybrid port, 133
- port-based VLAN trunk port, 133
- voice VLAN assignment mode (automatic), 175
- voice VLAN assignment mode (manual), 176

attribute
- Ethernet link aggregation attribute configuration, 39

auto
- interface auto power-down (Ethernet), 7
- interface automatic negotiation (Ethernet), 9
- loop detection port status auto recovery, 122
- voice VLAN assignment (automatic), 175
- voice VLAN assignment mode configuration (automatic), 183
- voice VLAN LLDP automatic IP phone discovery enable, 181
- voice VLAN port operation configuration (automatic assignment), 179

AutoMDIX mode (Ethernet interface), 13

B

backing up
MST backup port, 84
bandwidth
Ethernet link aggregate interface (expected bandwidth), 51
basic management LLDPDU TLV types, 236
BFD
Ethernet link aggregation group BFD, 52
blackhole
MAC address table entry, 20, 23
block action (loop detection), 122
boundary port (MST), 84
BPDU
MST region max hops, 92
spanning tree BPDU drop, 112
spanning tree BPDU guard, 109
spanning tree hello time, 93
spanning tree max age timer, 93
spanning tree TC-BPDU guard, 111
spanning tree TC-BPDU transmission restriction, 111
STP BPDU forwarding, 79
transmission rate configuration, 95
bridging
interface bridging enable (Layer 2 Ethernet), 14
LLDP agent customer bridge, 234
LLDP agent nearest bridge, 234
LLDP agent non-TPMR bridge, 234
MST common root bridge, 83
MST regional root, 83
spanning tree dispute guard, 112
spanning tree loop guard, 110
spanning tree root bridge, 91
spanning tree root bridge (device), 91
spanning tree root guard, 109
spanning tree secondary root bridge (device), 91
STP designated bridge, 74
STP root bridge, 73
bulk
interface configuration, 18, 18
interface configuration display, 19
interface configuration restrictions, 18

C

cable
interface cable connection (Layer 2 Ethernet), 14
calculating
MSTI calculation, 85
MSTP CIST calculation, 85
spanning tree port path cost calculation standard, 96
spanning tree timeout factor, 95
STP algorithm, 74
CDP
LLDP CDP compatibility, 247
LLDP CDP-compatible configuration, 254
voice VLAN advertisement, 181
voice VLAN information advertisement to IP phones, 174
changing
combo interface active port (Ethernet combo), 2
checking
spanning tree No Agreement Check, 105, 107
choosing
Ethernet link aggregation reference port, 40, 42
Cisco
Discovery Protocol. *Use* CDP
LLDP CDP compatibility, 247
LLDP configuration (CDP-compatible), 254
CIST
calculation, 85
network device connection, 83
spanning tree max age timer, 93
combining
interfaces (Ethernet 10-GE > 40-GE), 2
combo interface, 2
common root bridge, 83
configuring
1:1 VLAN mapping, 220, 226
1:2 VLAN mapping, 225, 231, 231
2:2 VLAN mapping, 225
authorization VLAN advertisement (CDP), 182
authorization VLAN advertisement (LLDP), 182
combo interface, 2
Ethernet aggregate interface, 49
Ethernet aggregate interface (description), 49
Ethernet aggregate interface (Layer 3 edge), 68
Ethernet link aggregate interface (Layer 2 edge), 64
Ethernet link aggregation, 38, 45, 58
Ethernet link aggregation (Layer 2 dynamic), 60
Ethernet link aggregation (Layer 2 static), 58
Ethernet link aggregation (Layer 3 dynamic), 67
Ethernet link aggregation (Layer 3 static), 66
Ethernet link aggregation edge aggregate interface, 51
Ethernet link aggregation group, 46
Ethernet link aggregation group (dynamic), 47

Ethernet link aggregation group (Layer 2 dynamic), 47
Ethernet link aggregation group (Layer 2 static), 46
Ethernet link aggregation group (Layer 3 dynamic), 48
Ethernet link aggregation group (Layer 3 static), 47
Ethernet link aggregation group (static), 46
Ethernet link aggregation group BFD, 52
Ethernet link aggregation group load sharing, 54
Ethernet link aggregation load sharing (Layer 2), 62
interface (Ethernet), 1
interface (inloopback), 17
interface (Layer 2 Ethernet), 9
interface (Layer 3 Ethernet), 14
interface (loopback), 16
interface (null), 16
interface basic settings (Ethernet), 3
interface card operating mode (Ethernet), 8
interface common settings (Ethernet), 1
interface generic flow control (Ethernet), 6
interface jumbo frame support (Ethernet), 4
interface link mode (Ethernet), 4
interface physical state change suppression (Ethernet), 5
interface storm control (Layer 2 Ethernet), 10
interface storm suppression (Ethernet), 9
interfaces in bulk, 18, 18
IP subnet-based VLAN, 139, 146
LLDP, 234, 240, 250
LLDP (CDP-compatible), 254
LLDP advertisable TLVs, 243
LLDP basics, 240, 250
LLDP CDP compatibility, 247
LLDP management address, 245
LLDP management address encoding format, 245
LLDP trapping, 248
LLDP-MED trapping, 248
loop detection, 121, 123, 125
loop detection protection action, 124
loop detection protection action (global), 124
loop detection protection action (Layer 2 aggregate interface), 124
loop detection protection action (Layer 2 Ethernet interface), 124
M:1 VLAN mapping, 220, 226
M:1 VLAN mapping (dynamic IP address assignment), 221
M:1 VLAN mapping (static IP address assignment), 223
M:1 VLAN mapping customer-side port (dynamic IP address assignment), 222
M:1 VLAN mapping customer-side port (static IP address assignment), 224
M:1 VLAN mapping network-side port (dynamic IP address assignment), 222
M:1 VLAN mapping network-side port (static IP address assignment), 224
MAC address table, 20, 21, 32
MAC address table entry, 22
MAC address table frame forwarding rule, 26
MAC address table multiport unicast entry (global), 24
MAC address table multiport unicast entry (on interface), 24
MAC Information, 34, 35
MAC Information mode, 34
MAC-based VLAN, 134, 144
MAC-based VLAN (server-assigned), 138
MAC-based VLAN assignment (dynamic), 138
MAC-based VLAN assignment (static), 137
management interface, 1
MST region, 90
MST region max hops, 92
MSTP, 88, 114
MVRP, 190, 193
port isolation, 70, 71
port-based VLAN, 131, 142
private VLAN, 156, 157, 159
private VLAN promiscuous port, 159
private VLAN trunk promiscuous port, 162
private VLAN trunk promiscuous+secondary port, 165
protocol-based VLAN, 140, 147
PVST, 88, 117
QinQ, 204, 210
QinQ basics, 210
QinQ CVLAN tag TPID value, 208
QinQ SVLAN tag TPID value, 208
QinQ VLAN tag TPID value, 207
QinQ VLAN transparent transmission, 206, 212
RSTP, 87
secondary VLAN Layer 3 communication, 170
service loopback group, 256, 257
spanning tree, 73, 86, 114
spanning tree BPDU transmission rate, 95
spanning tree device priority, 92
spanning tree Digest Snooping, 103, 104
spanning tree edge port, 95

spanning tree No Agreement Check, 105, 107
spanning tree port link type, 100
spanning tree port mode, 100
spanning tree port path cost, 96, 98
spanning tree port priority, 99
spanning tree port role restriction, 110
spanning tree protection functions, 108
spanning tree root bridge, 91
spanning tree root bridge (device), 91
spanning tree secondary root bridge, 91
spanning tree secondary root bridge (device), 91
spanning tree switched network diameter, 93
spanning tree TC Snooping, 107
spanning tree TC-BPDU transmission restriction, 111
spanning tree timeout factor, 95
spanning tree timer, 93
STP, 87
super VLAN, 151, 151, 153
super VLAN interface, 152
VLAN, 128, 142
VLAN basic settings, 129
VLAN group, 141
VLAN interface, 130
VLAN mapping, 214, 219, 226
voice VLAN, 173, 175, 183
voice VLAN advertisement (CDP), 181
voice VLAN advertisement (LLDP), 181
voice VLAN assignment mode (automatic), 183
voice VLAN assignment mode (manual), 185
voice VLAN port operation (automatic assignment), 179
voice VLAN port operation (manual assignment), 180
voice VLAN traffic QoS priority settings, 178
connecting
interface cable connection (Layer 2 Ethernet), 14
voice VLAN host+IP phone connection (in series), 175
voice VLAN IP phone+device, 175
CoS
voice VLAN traffic QoS priority settings, 178
cost
spanning tree port path cost calculation standard, 96
spanning tree port path cost configuration, 96, 98
STP path cost, 74
creating
super VLAN sub-VLAN, 151
CST
MST region connection, 83
CVLAN
QinQ basic configuration, 210
QinQ configuration, 204, 210
QinQ VLAN transparent transmission configuration, 212
VLAN mapping configuration, 214, 219, 226
VLAN mapping implementation, 216

D

default
Ethernet link aggregate interface default settings, 53
designated
MST port, 84
STP bridge, 74
STP port, 74
detecting
Ethernet link aggregation group BFD, 52
device
interface configuration (Ethernet), 1
LLDP basic configuration, 240, 250
LLDP CDP compatibility, 247
LLDP configuration, 234, 240, 250
LLDP configuration (CDP-compatible), 254
LLDP parameters, 246
loop protection actions, 122
MSTP implementation, 85
MVRP configuration, 187, 190, 193
spanning tree BPDU drop, 112
spanning tree BPDU guard, 109
spanning tree Digest Snooping, 103, 104
spanning tree dispute guard, 112
spanning tree loop guard, 110
spanning tree No Agreement Check, 105, 107
spanning tree port role restriction, 110
spanning tree priority, 92
spanning tree protection functions, 108
spanning tree root guard, 109
spanning tree TC Snooping, 107
spanning tree TC-BPDU guard, 111
spanning tree TC-BPDU transmission restriction, 111
voice VLAN IP phone+device connection, 175
DHCP snooping
M:1 VLAN mapping, 221
Digest Snooping (spanning tree), 103, 104
directing
Ethernet link aggregation traffic redirection, 56

disabling
MAC address learning, 24
MAC address learning (global), 24
MAC address learning (on interface), 25
MAC address learning (on VLAN), 25
discarding
MST discarding port state, 84
displaying
bulk interface configuration, 19
Ethernet link aggregation, 58
interface, 17
interface (Ethernet), 15
LLDP, 249
loop detection, 125
MAC address table, 31
MVRP, 193
port isolation, 70
private VLAN, 159
QinQ, 209
service loopback group, 256
spanning tree, 113
super VLAN, 152
VLAN, 142
VLAN mapping, 226
voice VLAN, 183
dispute
spanning tree dispute guard, 112
dot1d-1998 (STP port path cost calculation), 96
dot1s (STP port mode), 100
dot1t (STP port path cost calculation), 96
downgrading
interface automatic negotiation (Ethernet), 9
DSCP
voice VLAN traffic QoS priority settings, 178
dynamic
Ethernet link aggregation (dynamic mode), 41
Ethernet link aggregation (Layer 2), 60
Ethernet link aggregation (Layer 3), 67
Ethernet link aggregation edge aggregate interface, 45
Ethernet link aggregation group, 47
Ethernet link aggregation group BFD, 52
Ethernet link aggregation mode, 40
Layer 2 Ethernet link aggregation group, 47
Layer 3 Ethernet link aggregation group, 48
MAC address table dynamic aging timer, 25
MAC address table entry, 20
MAC address table entry configuration (global), 22
MAC address table entry configuration (on interface), 22
MAC-based VLAN assignment, 135, 138

E

edge
Ethernet aggregate interface (Layer 3 edge), 68
Ethernet link aggregate interface (Layer 2 edge), 64
edge port
MST, 84
spanning tree, 95
EEE energy saving, 8
enabling
Ethernet link aggregation traffic redirection, 56
interface auto power-down (Ethernet), 7
interface automatic negotiation (Ethernet), 9
interface bridging (Layer 2 Ethernet), 14
interface EEE (Ethernet), 8
interface energy-saving features (Ethernet), 7
interface loopback testing (Ethernet), 6
LLDP, 240
LLDP polling, 242
loop detection (global), 123
loop detection (port-specific), 123
M:1 VLAN mapping ARP detection (dynamic IP address assignment), 221
M:1 VLAN mapping ARP snooping (static IP address assignment), 223
M:1 VLAN mapping DHCP snooping (dynamic IP address assignment), 221
MAC address move notification, 29
MAC address synchronization, 28
MAC address table ARP fast update, 30
MAC address table SNMP notification, 31
MAC Information, 34
MVRP, 191
MVRP GVRP compatibility, 193
QinQ, 206
spanning tree BPDU drop, 112
spanning tree BPDU guard, 109
spanning tree dispute guard, 112
spanning tree feature, 101
spanning tree loop guard, 110
spanning tree port state transition information output, 101
spanning tree root guard, 109
spanning tree TC-BPDU guard, 111
voice VLAN LLDP automatic IP phone discovery, 181
encapsulating
LLDP frame encapsulation (Ethernet II), 235
LLDP frame encapsulation (SNAP), 235
LLDP frame encapsulation format, 246

VLAN frame encapsulation, 128
Energy Efficient Ethernet. *See EEE*
energy-saving features, 7
Ethernet
interface. *See* Ethernet interface
interface auto power-down enable, 7
interface dampening restrictions, 6
interface display, 15
interface EEE enable, 8
interface energy-saving features, 7
interface generic flow control, 6
interface loopback testing, 6
interface maintain, 15
interface physical state change suppression, 5
link aggregation. *See* Ethernet link aggregation
LLDP frame encapsulation, 235
LLDP trapping, 248
LLDP-MED trapping, 248
loop detection configuration, 121, 125
loop detection protection action (Layer 2 Ethernet interface), 124
MAC address table configuration, 20, 21, 32
MAC Information configuration, 34, 35
port isolation configuration, 70, 71
port-based VLAN assignment (access port), 132
port-based VLAN assignment (hybrid port), 133
port-based VLAN assignment (trunk port), 133
port-based VLAN configuration, 131
private VLAN configuration, 156, 157, 159
private VLAN promiscuous port configuration, 159
private VLAN trunk promiscuous port configuration, 162
private VLAN trunk promiscuous+secondary port configuration, 165
QinQ CVLAN frame header tag, 204
QinQ SVLAN frame header tag, 204
secondary VLAN Layer 3 communication configuration, 170
service loopback group configuration, 256, 257
subinterface. *See Ethernet interface, Ethernet subinterface, subinterface*
super VLAN configuration, 151, 151, 153
super VLAN sub-VLAN creation, 151
VLAN basic configuration, 129
VLAN configuration, 128, 142
VLAN frame encapsulation, 128
VLAN interface, 130
VLAN port-based configuration, 142
voice VLAN configuration, 173, 175, 183
Ethernet interface
10-GE > 40-GE combine;010-GE > 40-GE combine, 2
40-GE split;040-GE split, 2
automatic negotiation enable, 9
basic settings configuration, 3
bridging enable (Layer 2), 14
cable connection (Layer 2), 14
combo interface active port, 2
combo interface configuration, 2
common settings configuration, 1
configuration, 1
configuration (Layer 2), 9
configuration (Layer 3), 14
fiber port (Layer 2), 12
fiber port restrictions (Layer 2), 12
interface card operating mode, 8
jumbo frame support configuration, 4
link mode, 4
management interface configuration, 1
MDIX mode (Layer 2), 13
MTU setting (Layer 3), 14
naming conventions, 1
statistics polling interval, 8
storm control (Layer 2), 10
storm suppression, 9
Ethernet link aggregation
aggregate group Selected ports min/max, 50
aggregate interface, 38
aggregate interface (description), 49
aggregate interface configuration, 49
aggregate interface default settings, 53
aggregate interface shutdown, 53
aggregation group, 38
aggregation group restrictions, 46
basic concepts, 38
BFD configuration, 52
BFD configuration restrictions, 52
configuration, 38, 45, 58
configuration types, 39
display, 58
dynamic mode, 41
edge aggregate interface, 45, 51
group (Layer 3 dynamic), 48
group (Layer 3 static), 47
group configuration, 46
group configuration (dynamic), 47
group configuration (static), 46

group load sharing configuration, 54
group load sharing mode, 54
how dynamic link aggregation works, 42
interface configuration (expected bandwidth), 51
LACP, 41
Layer 2 aggregate interface (ignored VLAN), 50, 50
Layer 2 aggregate interface (Layer 2 edge), 64
Layer 2 aggregation configuration (dynamic), 60
Layer 2 aggregation configuration (static), 58
Layer 2 aggregation load sharing (Layer 2), 62
Layer 2 group (dynamic), 47
Layer 2 group (static), 46
Layer 3 aggregate interface (Layer 3 edge), 68
Layer 3 aggregate interface configuration (MTU), 50
Layer 3 aggregation configuration (dynamic), 67
Layer 3 aggregation configuration (static), 66
load sharing mode, 45
local-first load sharing, 55
maintain, 58
management VLAN+management port, 57
member port, 38
member port state, 38, 40, 43
modes, 40
operational key, 39
per-flow load sharing algorithm settings, 55
reference port, 42
reference port choice, 40
static mode, 40
traffic redirection, 56
traffic redirection restrictions, 56
Ethernet subinterface, 1, *See also Ethernet interface, Layer 2 Ethernet subinterface, Layer 3 Ethernet subinterface*
external
interface external loopback testing (Ethernet), 6

F

fast
MAC address table ARP fast update, 30
fiber port
interface fiber port (Layer 2 Ethernet), 12
flow control
interface generic flow control (Ethernet), 6
forcing
interface fiber port (Layer 2 Ethernet), 12
format
LLDP frame encapsulation (Ethernet II), 235
LLDP frame encapsulation (SNAP), 235
LLDP frame encapsulation format, 246
LLDP management address encoding format, 245
forwarding
MAC address table frame forwarding rule, 26
MST forwarding port state, 84
spanning tree forward delay timer, 93
STP BPDU forwarding, 79
STP forward delay timer, 79
frame
interface jumbo frame support (Ethernet), 4
LLDP frame encapsulation format, 246
loop detection (Ethernet frame header), 121
loop detection (inner frame header), 121
loop detection interval, 122
MAC address learning, 20
MAC address table blackhole entry, 23
MAC address table configuration, 20, 21, 32
MAC address table entry configuration, 22
MAC address table frame forwarding rule, 26
MAC address table multiport unicast entry, 23
MAC Information configuration, 34, 35
port-based VLAN frame handling, 131
QinQ CVLAN Ethernet frame header tag, 204
QinQ implementation, 205
QinQ SVLAN Ethernet frame header tag, 204
VLAN frame encapsulation, 128

G

GARP
VLAN Registration Protocol. *Use* GVRP
generic flow control (Ethernet interface), 6
Generic VLAN Registration Protocol. *Use* GVRP
global
Ethernet link aggregation load sharing mode set, 54
loop detection enable, 123
loop detection protection action, 124
MAC address learning disable, 24
MAC address table multiport unicast entry configuration, 24
group
Ethernet link aggregate group Selected ports min/max, 50
Ethernet link aggregation, 46
Ethernet link aggregation group, 38
Ethernet link aggregation group (dynamic), 47

Ethernet link aggregation group (Layer 2 static), 46, 47
Ethernet link aggregation group (Layer 3 dynamic), 48
Ethernet link aggregation group (Layer 3 static), 47
Ethernet link aggregation group (static), 46
Ethernet link aggregation group load sharing, 54
Ethernet link aggregation LACP, 41
Ethernet link aggregation load sharing mode, 45, 54
Ethernet link aggregation member port state, 38
VLAN group configuration, 141
GVRP
MVRP compatibility, 193

H

hello
spanning tree timer, 93
STP timer, 79
host
voice VLAN host+IP phone connection (in series), 175
voice VLAN IP phone+device connection, 175
hybrid port
port-based VLAN assignment (hybrid port), 133

I

identifying
voice VLAN IP phone identification (LLDP), 174
voice VLAN IP phone identification (OUI address), 173
ignored VLAN
Layer 2 aggregate interface, 50
implementing
1:1 VLAN mapping, 216, 217
1:2 VLAN mapping, 216, 218
2:2 VLAN mapping, 216, 218
M:1 VLAN mapping, 216, 217
MSTP device implementation, 85
QinQ, 205
inloopback interface
configuration, 17
display, 17
maintain, 17
interface
bulk configuration, 18, 18
configuration (inloopback), 16, 17
configuration (loopback), 16, 16
configuration (null), 16, 16
Ethernet aggregate interface, 49
Ethernet aggregate interface (description), 49
Ethernet link aggregate interface default settings, 53
Ethernet link aggregate interface shutdown, 53
Ethernet link aggregation edge aggregate interface, 45, 51
Layer 2 Ethernet aggregate interface (ignored VLAN), 50
Layer 3 aggregate interface configuration (MTU), 50
internal
interface internal loopback testing (Ethernet), 6
interval
Ethernet link aggregation LACP long timeout, 42
Ethernet link aggregation LACP short timeout, 42
loop detection, 122, 124
MAC change notification interval, 35
IP addressing
IP subnet-based VLAN configuration, 139, 146
super VLAN configuration, 151, 151, 153
super VLAN interface configuration, 152
voice VLAN configuration, 173, 175, 183
IP phone
voice VLAN assignment mode+IP phone cooperation, 176
voice VLAN host+IP phone connection (in series), 175
voice VLAN identification (LLDP), 174
voice VLAN identification (OUI address), 173
voice VLAN information advertisement, 174
voice VLAN IP phone access method, 175
voice VLAN IP phone+device connection, 175
IP subnet-based VLAN
configuration, 139, 146
isolating
ports. *See* port isolation
IST
MST region, 83

J

jumbo frame support (Ethernet interface), 4

K

key
Ethernet link aggregation operational key, 39

L

LACP
Ethernet link aggregation, 41
LAN

Virtual Local Area Network. *Use* VLAN
LAN switching
1:1 VLAN mapping configuration, 220, 226
1:2 VLAN mapping configuration, 225, 231
2:2 VLAN mapping configuration, 225, 231
authorization VLAN advertisement (CDP), 182
authorization VLAN advertisement (LLDP), 182
Ethernet aggregate interface, 49
Ethernet aggregate interface (description), 49
Ethernet aggregate interface (ignored VLAN), 50
Ethernet aggregate interface (Layer 3 edge), 68
Ethernet link aggregate group Selected ports min/max, 50
Ethernet link aggregate interface (expected bandwidth), 51
Ethernet link aggregate interface (Layer 2 edge), 64
Ethernet link aggregate interface default settings, 53
Ethernet link aggregate interface shutdown, 53
Ethernet link aggregation (dynamic mode), 41
Ethernet link aggregation (Layer 2 dynamic), 60
Ethernet link aggregation (Layer 2 static), 58
Ethernet link aggregation (Layer 3 dynamic), 67
Ethernet link aggregation (Layer 3 static), 66
Ethernet link aggregation (static mode), 40
Ethernet link aggregation basic concepts, 38
Ethernet link aggregation BFD configuration restrictions, 52
Ethernet link aggregation configuration, 38, 45, 58
Ethernet link aggregation display, 58
Ethernet link aggregation edge aggregate interface, 45, 51
Ethernet link aggregation group, 46
Ethernet link aggregation group (dynamic dynamic), 47
Ethernet link aggregation group (dynamic), 47
Ethernet link aggregation group (Layer 2 static), 46
Ethernet link aggregation group (Layer 3 dynamic), 48
Ethernet link aggregation group (Layer 3 static), 47
Ethernet link aggregation group (static), 46
Ethernet link aggregation group load sharing, 54
Ethernet link aggregation group load sharing mode, 54
Ethernet link aggregation group restrictions, 46
Ethernet link aggregation LACP, 41
Ethernet link aggregation load sharing (Layer 2), 62
Ethernet link aggregation load sharing mode, 45
Ethernet link aggregation local-first load sharing, 55
Ethernet link aggregation maintain, 58
Ethernet link aggregation traffic redirection, 56
Ethernet link aggregation traffic redirection restrictions, 56
IP subnet-based VLAN configuration, 139, 146
LLDP basic concepts, 234
LLDP basic configuration, 240, 250
LLDP CDP compatibility, 247
LLDP configuration, 234, 240, 250
LLDP configuration (CDP-compatible), 254
LLDP display, 249
LLDP protocols and standards, 240
loop detection configuration, 121, 123, 125
M:1 VLAN mapping configuration, 220, 226
M:1 VLAN mapping restrictions (dynamic IP address assignment), 221
M:1 VLAN mapping restrictions (static IP address assignment), 223
MAC address table configuration, 20, 21, 32
MAC address table display, 31
MAC Information configuration, 34, 35
MAC-based VLAN assignment (dynamic), 138
MAC-based VLAN assignment (static), 137
MAC-based VLAN assignment configuration restrictions (dynamic), 180
MAC-based VLAN configuration, 134, 144
MAC-based VLAN configuration (server-assigned), 138
MRP implementation, 187
MVRP configuration, 187, 190, 193
MVRP configuration restrictions, 190
MVRP display, 193
MVRP GVRP compatibility, 193
MVRP maintain, 193
MVRP protocols and standards, 190
MVRP registration mode setting, 192
MVRP timer set, 192
port isolation configuration, 70, 71
port isolation display, 70
port isolation group assignment (multiple ports), 70
port-based VLAN assignment (access port), 132
port-based VLAN assignment (hybrid port), 133

port-based VLAN assignment (trunk port), 133
port-based VLAN configuration, 131
private VLAN configuration, 157, 159
private VLAN configuration restrictions, 157
private VLAN display, 159
private VLAN promiscuous port configuration, 159
private VLAN trunk promiscuous port configuration, 162
private VLAN trunk promiscuous+secondary port configuration, 165
protocol-based VLAN configuration, 140, 147
QinQ basic configuration, 210
QinQ configuration, 204, 210
QinQ configuration restrictions, 206
QinQ CVLAN tag TPID value, 208
QinQ implementation, 205
QinQ protocols and standards, 205
QinQ SVLAN tag 802.1p priority, 208
QinQ SVLAN tag TPID value, 208
QinQ VLAN tag TPID value, 207
QinQ VLAN transparent transmission configuration, 212
secondary VLAN Layer 3 communication configuration, 170
service loopback group configuration, 256, 257
service loopback group display, 256
super VLAN configuration, 151, 151, 153
super VLAN display, 152
super VLAN interface configuration, 152
super VLAN sub-VLAN creation, 151
VLAN basic configuration, 129
VLAN configuration, 128, 142
VLAN display, 142
VLAN group configuration, 141
VLAN interface, 130
VLAN maintain, 142
VLAN mapping configuration, 214, 219, 226
VLAN mapping display, 226
VLAN port-based configuration, 142
VLAN protocols and standards, 129
voice VLAN advertisement (CDP), 181
voice VLAN advertisement (LLDP), 181
voice VLAN assignment mode configuration (automatic), 183
voice VLAN assignment mode configuration (manual), 185
voice VLAN display, 183
voice VLAN LLDP automatic IP phone discovery enable, 181
voice VLAN port operation configuration (automatic assignment), 179
voice VLAN port operation configuration (manual assignment), 180
voice VLAN port operation configuration restrictions (automatic assignment), 137
voice VLAN port operation configuration restrictions (manual assignment), 181

Layer 2
Ethernet interface bridging enable, 14
Ethernet interface cable connection, 14
Ethernet interface configuration, 9
Ethernet interface fiber port, 12
Ethernet interface fiber port restrictions, 12
Ethernet interface MDIX mode, 13
Ethernet interface storm control configuration, 10
Ethernet link aggregate interface (Layer 2 edge), 64
Ethernet link aggregation (Layer 2 dynamic), 60
Ethernet link aggregation (Layer 2 static), 58
Ethernet link aggregation load sharing, 62
interface configuration (Ethernet), 1
LLDP basic configuration, 250
LLDP configuration, 250
LLDP trapping, 248
LLDP-MED trapping, 248
loop detection protection action (Layer 2 aggregate interface), 124
loop detection protection action (Layer 2 Ethernet interface), 124
VLAN basic configuration, 129
VLAN configuration, 128, 142
voice VLAN configuration, 173, 175, 183

Layer 2 LAN switching
displaying spanning tree, 113
maintaining spanning tree, 113
MST region, 90
MSTP configuration, 114
private VLAN configuration, 156
PVST configuration, 117
spanning tree configuration, 73, 114
spanning tree Digest Snooping, 103, 104

Layer 3
aggregate interface configuration (MTU), 50
Ethernet aggregate interface, 49
Ethernet aggregate interface (description), 49
Ethernet aggregate interface (Layer 3 edge), 68
Ethernet interface MTU setting, 14
Ethernet link aggregate group Selected ports min/max, 50
Ethernet link aggregate interface (expected bandwidth), 51

Ethernet link aggregate interface default settings, 53
Ethernet link aggregate interface shutdown, 53
Ethernet link aggregation (Layer 3 dynamic), 67
Ethernet link aggregation (Layer 3 static), 66
Ethernet link aggregation configuration, 38, 45, 58
Ethernet link aggregation edge aggregate interface, 45, 51
Ethernet link aggregation group, 46
Ethernet link aggregation group (dynamic), 47
Ethernet link aggregation group (static), 46
Ethernet link aggregation group load sharing, 54
Ethernet link aggregation group load sharing mode, 54
Ethernet link aggregation local-first load sharing, 55
Ethernet link aggregation traffic redirection, 56
interface configuration, 14
interface configuration (Ethernet), 1
IP subnet-based VLAN configuration, 139
LAN switching LAN switching VLAN interface, 130
LLDP basic configuration, 250
LLDP configuration, 250
LLDP trapping, 248
LLDP-MED trapping, 248
port-based VLAN assignment (access port), 132
port-based VLAN assignment (hybrid port), 133
port-based VLAN assignment (trunk port), 133
port-based VLAN configuration, 131
private VLAN configuration, 159
private VLAN promiscuous port configuration, 159
private VLAN trunk promiscuous port configuration, 162
private VLAN trunk promiscuous+secondary port configuration, 165
protocol-based VLAN configuration, 140
secondary VLAN Layer 3 communication configuration, 170
super VLAN configuration, 153
voice VLAN configuration, 173, 175, 183
learning
loop detection no-learning action, 122
MAC address, 20
MAC address learning disable, 24
MAC address table learning limit, 26
MAC address table learning priority, 27
MST learning port state, 84
legacy
spanning tree port mode, 100
spanning tree port path cost calculation, 96
link
aggregation. *See* link aggregation
interface link mode (Ethernet), 4
Link Layer Discovery Protocol. *Use* LLDP
MSTP configuration, 114
PVST configuration, 117
spanning tree configuration, 73, 86, 114
spanning tree hello time, 93
spanning tree port link type configuration, 100
link aggregation
Ethernet link aggregation. *See* Ethernet link aggregation
LLDP
advertisable TLV configuration, 243
agent, 234
basic concepts, 234
basic configuration, 240, 250
CDP compatibility configuration, 247
CDP-compatible configuration, 254
configuration, 234, 240, 250
display, 249
enable, 240
frame encapsulation (Ethernet II), 235
frame encapsulation (SNAP), 235
frame encapsulation format, 246
frame format, 235
frame reception, 240
frame transmission, 239
how it works, 239
LLDPDU management address TLV, 239
LLDPDU TLV types, 236
LLDPDU TLVs, 236
LLDP-MED trapping configuration, 248
management address configuration, 245
management address encoding format, 245
operating mode (disable), 239
operating mode (Rx), 239
operating mode (Tx), 239
operating mode (TxRx), 239
operating mode set, 242
parameter set, 246
polling enable, 242
protocols and standards, 240
reinitialization delay, 242

trapping configuration, 248
voice VLAN advertisement, 181
voice VLAN information advertisement to IP phones, 174
voice VLAN IP phone identification, 174
voice VLAN IP phone identification method, 173
voice VLAN LLDP automatic IP phone discovery enable, 181
LLDPDU
LLDP basic configuration, 240, 250
LLDP configuration, 234, 240, 250
LLDP parameters, 246
management address configuration, 245
management address encoding format, 245
management address TLV, 239
TLV basic management types, 236
TLV LLDP-MED types, 236
TLV organization-specific types, 236
load balancing
service loopback group configuration, 256, 257
load sharing
Ethernet link aggregation group configuration, 54
Ethernet link aggregation group load sharing, 45
Ethernet link aggregation load sharing (Layer 2), 62
Ethernet link aggregation load sharing mode, 54
Ethernet link aggregation local-first load sharing, 55
Ethernet link aggregation packet type-based load sharing, 45
Ethernet link aggregation per-flow load sharing, 45
Ethernet link aggregation per-flow load sharing algorithm settings, 55
Ethernet link aggregation per-packet load sharing, 45
local
Ethernet link aggregation local-first load sharing, 55
Ethernet link aggregation per-flow load sharing algorithm settings, 55
loop
MSTP configuration, 114
PVST configuration, 117
spanning tree configuration, 73, 86, 114
spanning tree loop guard, 110
loop detection
configuration, 121, 123, 125
display, 125
enable, 123
enable (global), 123
enable (port-specific), 123
interval, 122
interval setting, 124
mechanisms, 121
port status auto recovery, 122
protection action configuration, 124
protection action configuration (global), 124
protection action configuration (Layer 2 aggregate interface), 124
protection action configuration (Layer 2 Ethernet interface), 124
protection actions, 122
loopback
interface loopback testing (Ethernet), 6
loopback interface
configuration, 16
display, 17
maintain, 17

M

M:1 VLAN mapping
application scenario, 214
ARP detection (dynamic IP address assignment), 221
ARP snooping (static IP address assignment), 223
configuration, 220, 226
configuration (dynamic IP address assignment), 221
configuration (static IP address assignment), 223
configuration restrictions (dynamic IP address assignment), 221
configuration restrictions (static IP address assignment), 223
customer-side port (dynamic IP address assignment), 222
customer-side port (static IP address assignment), 224
DHCP snooping (dynamic IP address assignment), 221
implementation, 216, 217
network-side port (dynamic IP address assignment), 222
network-side port (static IP address assignment), 224
MAC address table
address learning, 20
address synchronization, 28

ARP fast update enable, 30
blackhole entry, 23
configuration, 20, 21, 32
display, 31
dynamic aging timer, 25
entry configuration, 22
entry configuration (global), 22
entry configuration (on interface), 22
entry creation, 20
entry types, 20
frame forwarding rule, 26
learning limit set, 26
learning priority assignment, 27
MAC address learning disable, 24
MAC address move notification, 29
manual entries, 20
multiport unicast entry, 23
SNMP notification enable, 31
MAC addressing
MAC-based VLAN assignment (dynamic), 135, 138
MAC-based VLAN assignment (server-assigned), 136
MAC-based VLAN assignment (static), 134, 137
MAC-based VLAN configuration, 134, 144
MAC-based VLAN configuration (server-assigned), 138
VLAN frame encapsulation, 128
MAC Information
change notification interval, 35
configuration, 34, 35
configuration restrictions, 36
enable, 34
mode configuration, 34
queue length setting, 35
MAC relay (LLDP agent), 234
MAC-based VLAN
assignment (dynamic), 138
assignment (static), 137
configuration, 134, 144
configuration (server-assigned), 138
dynamic assignment, 135
dynamic assignment configuration restrictions, 180
server-assigned, 136
static assignment, 134
maintaining
Ethernet link aggregation, 58
interface, 17
interface (Ethernet), 15
MVRP, 193
spanning tree, 113
VLAN, 142
management address
LLDP encoding format, 245
manual
voice VLAN assignment mode, 176
voice VLAN assignment mode configuration, 185
voice VLAN port operation configuration, 180
mapping
1:1 VLAN mapping, 214
1:2 VLAN mapping, 216
2:2 VLAN mapping, 216
M:1 VLAN mapping, 214
MSTP VLAN-to-instance mapping table, 83
master
MSTP master port, 84
max age timer (STP), 79
mCheck
spanning tree, 102
MDI mode (Ethernet interface), 13
MDIX mode (Ethernet interface), 13
MED (LLDP-MED trapping), 248
message
MRP JoinEmpty, 187
MRP JoinIn, 187
MRP Leave, 187
MRP LeaveAll, 187
MRP New, 187
MRP timers, 189
MIB
LLDP basic configuration, 240, 250
LLDP configuration, 234, 240, 250
mode
Ethernet link aggregation dynamic, 40, 41
Ethernet link aggregation LACP operation active, 42
Ethernet link aggregation LACP operation passive, 42
Ethernet link aggregation load sharing, 45
Ethernet link aggregation static, 40, 40
interface Auto MDIX (Layer 2 Ethernet), 13
interface link (Ethernet), 4
interface MDI (Layer 2 Ethernet), 13
interface MDIX (Layer 2 Ethernet), 13
LLDP disable, 239, 242
LLDP Rx, 239, 242
LLDP Tx, 239, 242
LLDP TxRx, 239, 242
MAC Information syslog, 34
MAC Information trap, 34

MVRP registration, 192
MVRP registration fixed, 190
MVRP registration forbidden, 190
MVRP registration normal, 190
spanning tree mCheck, 102
spanning tree MSTP, 89
spanning tree PVST, 89
spanning tree RSTP, 89
spanning tree STP, 89
voice VLAN assignment automatic, 175
voice VLAN assignment manual, 176
voice VLAN port normal, 177
voice VLAN port security, 177
modifying
MAC address table blackhole entry, 23
MAC address table entry (global), 22
MAC address table entry (on interface), 22
MAC address table multiport unicast entry, 23
MRP
implementation, 187
messages, 187
MVRP configuration, 187, 190, 193
timers, 189
MST
region max hops, 92
MSTI
calculation, 85
MRP, 187
MST instance, 83
MSTP, 73, *See also* STP
basic concepts, 81
CIST, 83
CIST calculation, 85
common root bridge, 83
configuration, 88, 114
CST, 83
device implementation, 85
feature enable, 102
features, 81
how it works, 85
IST, 83
mode set, 89
MST region, 82
MST region configuration, 90
MSTI, 83
MSTI calculation, 85
port roles, 84
port states, 84
protocols and standards, 86
regional root, 83
relationships, 80
spanning tree max age timer, 93
spanning tree port mode configuration, 100
VLAN-to-instance mapping table, 83
MTU
Layer 3 Ethernet aggregate interface, 50
multiple
Registration Protocol. *Use* MRP
VLAN Registration Protocol. *Use* MVRP
Multiple Spanning Tree Protocol. *Use* MSTP
multiport unicast entry (MAC address table), 20, 23
MVRP
configuration, 187, 190, 193
configuration restrictions, 190
display, 193
enable, 191
GVRP compatibility, 193
maintain, 193
MRP implementation, 187
protocols and standards, 190
registration mode setting, 192
registration modes, 190
timer set, 192

N

negotiating
interface automatic negotiation (Ethernet), 9
network
1:1 VLAN mapping configuration, 220, 226
1:2 VLAN mapping configuration, 225, 231
2:2 VLAN mapping configuration, 225, 231
authorization VLAN advertisement (CDP), 182
authorization VLAN advertisement (LLDP), 182
combo interface configuration, 2
Ethernet aggregate interface (Layer 3 edge), 68
Ethernet link aggregate interface (Layer 2 edge), 64
Ethernet link aggregation (dynamic mode), 41
Ethernet link aggregation (Layer 2 dynamic), 60
Ethernet link aggregation (Layer 2 static), 58
Ethernet link aggregation (Layer 3 dynamic), 67
Ethernet link aggregation (Layer 3 static), 66
Ethernet link aggregation (static mode), 40
Ethernet link aggregation configuration types, 39
Ethernet link aggregation edge aggregate interface, 45
Ethernet link aggregation LACP, 41
Ethernet link aggregation load sharing (Layer 2), 62
Ethernet link aggregation member port state, 40, 43

Ethernet link aggregation modes, 40
Ethernet link aggregation operational key, 39
Ethernet link aggregation reference port, 42
Ethernet link aggregation reference port choice, 40
interface auto power-down (Ethernet), 7
interface automatic negotiation (Ethernet), 9
interface basic settings (Ethernet), 3
interface bridging enable (Layer 2 Ethernet), 14
interface cable connection (Layer 2 Ethernet), 14
interface card operating mode (Ethernet), 8
interface common settings configuration (Ethernet), 1
interface configuration (inloopback), 17
interface configuration (Layer 2 Ethernet), 9
interface configuration (Layer 3 Ethernet), 14
interface configuration (loopback), 16
interface configuration (null), 16
interface EEE (Ethernet), 8
interface energy-saving features (Ethernet), 7
interface fiber port (Layer 2 Ethernet), 12
interface generic flow control (Ethernet), 6
interface jumbo frame support (Ethernet), 4
interface link mode (Ethernet), 4
interface loopback testing (Ethernet), 6
interface MDIX mode (Layer 2 Ethernet), 13
interface MTU setting (Layer 3 Ethernet), 14
interface physical state change suppression (Ethernet), 5
interface split (Ethernet 40-GE), 2
interface statistics polling interval (Ethernet), 8
interface storm control (Layer 2 Ethernet), 10
interface storm suppression (Ethernet), 9
interfaces combine (Ethernet 10-GE > 40-GE), 2
IP subnet-based VLAN configuration, 139, 146
LLDP basic configuration, 240, 250
LLDP configuration (CDP-compatible), 254
loop detection enable, 123
loop detection interval, 122, 124
loop detection protection action configuration, 124
loop protection actions, 122
M:1 VLAN mapping configuration, 220, 226
M:1 VLAN mapping configuration (dynamic IP address assignment), 221
M:1 VLAN mapping configuration (static IP address assignment), 223
M:1 VLAN mapping customer-side port (dynamic IP address assignment), 222
M:1 VLAN mapping customer-side port (static IP address assignment), 224
M:1 VLAN mapping network-side port (dynamic IP address assignment), 222
M:1 VLAN mapping network-side port (static IP address assignment), 224
MAC address move notification, 29
MAC address table address synchronization, 28
MAC address table ARP fast update, 30
MAC address table blackhole entry, 23
MAC address table dynamic aging timer, 25
MAC address table entry configuration, 22
MAC address table entry types, 20
MAC address table learning limit, 26
MAC address table learning priority, 27
MAC address table multiport unicast entry, 23
MAC address table SNMP notification, 31
MAC Information configuration, 35
MAC-based VLAN assignment (dynamic), 138
MAC-based VLAN assignment (server-assigned), 136
MAC-based VLAN assignment (static), 137
MAC-based VLAN configuration, 134, 144
MAC-based VLAN configuration (server-assigned), 138
management interface configuration, 1
MRP timers, 189
MST region configuration, 90
MVRP timer set, 192
port isolation group assignment (multiple ports), 70
port-based VLAN assignment (access port), 132
port-based VLAN assignment (hybrid port), 133
port-based VLAN assignment (trunk port), 133
port-based VLAN configuration, 131
private VLAN promiscuous port configuration, 159
private VLAN trunk promiscuous port configuration, 162
private VLAN trunk promiscuous+secondary port configuration, 165
protocol-based VLAN configuration, 140, 147
QinQ basic configuration, 210
QinQ CVLAN tag TPID value, 208
QinQ SVLAN tag TPID value, 208
QinQ VLAN tag TPID value, 207
QinQ VLAN transparent transmission, 206
QinQ VLAN transparent transmission configuration, 212
RSTP network convergence, 80

secondary VLAN Layer 3 communication configuration, 170
service loopback group configuration, 257
spanning tree BPDU drop, 112
spanning tree BPDU guard, 109
spanning tree BPDU transmission rate, 95
spanning tree Digest Snooping, 103, 104
spanning tree dispute guard, 112
spanning tree edge port, 95
spanning tree loop guard, 110
spanning tree mode set, 89
spanning tree No Agreement Check, 105, 107
spanning tree port link type, 100
spanning tree port mode, 100
spanning tree port path cost, 96, 98
spanning tree port priority, 99
spanning tree port role restriction, 110
spanning tree port state transition, 101
spanning tree priority, 92
spanning tree protection functions, 108
spanning tree root bridge, 91
spanning tree root bridge (device), 91
spanning tree root guard, 109
spanning tree secondary root bridge (device), 91
spanning tree switched network diameter, 93
spanning tree TC Snooping, 107
spanning tree TC-BPDU guard, 111
spanning tree TC-BPDU transmission restriction, 111
STP algorithm calculation, 74
STP designated bridge, 74
STP designated port, 74
STP path cost, 74
STP root bridge, 73
STP root port, 74
super VLAN configuration, 151, 153
super VLAN interface configuration, 152
super VLAN sub-VLAN creation, 151
VLAN basic configuration, 129
VLAN group configuration, 141
VLAN interface, 130
VLAN mapping 1:1 implementation, 217
VLAN mapping 1:2 implementation, 218
VLAN mapping 2:2 implementation, 218
VLAN mapping M:1 implementation, 217
VLAN port-based configuration, 142
voice VLAN advertisement (CDP), 181
voice VLAN advertisement (LLDP), 181
voice VLAN assignment mode, 175
voice VLAN assignment mode configuration (automatic), 183
voice VLAN assignment mode configuration (manual), 185
voice VLAN configuration, 183
voice VLAN host+IP phone connection (in series), 175
voice VLAN information advertisement to IP phones, 174
voice VLAN IP phone access method, 175
voice VLAN IP phone identification (LLDP), 174
voice VLAN IP phone identification (OUI address), 173
voice VLAN IP phone+device connection, 175
voice VLAN LLDP automatic IP phone discovery enable, 181
voice VLAN port mode, 177
voice VLAN port operation configuration (automatic assignment), 179
voice VLAN port operation configuration (manual assignment), 180
voice VLAN traffic QoS priority settings, 178
network management
Ethernet link aggregation basic concepts, 38
Ethernet link aggregation configuration, 38, 45, 58
interface bulk configuration, 18, 18
interface configuration (Ethernet), 1
interface configuration (inloopback), 16
interface configuration (loopback), 16
interface configuration (null), 16
LLDP basic concepts, 234
LLDP configuration, 234, 240, 250
loop detection, 121
loop detection configuration, 123, 125
MAC address table configuration, 20, 21, 32
MAC Information configuration, 34
MSTP configuration, 114
MVRP, 187, 190, 193
port isolation configuration, 70, 71
private VLAN configuration, 156, 157, 159
PVST configuration, 117
QinQ configuration, 204, 210
service loopback group configuration, 256
spanning tree configuration, 73, 86, 114
super VLAN configuration, 151
VLAN configuration, 128, 142
VLAN mapping configuration, 214, 219, 226
voice VLAN configuration, 173, 175
No Agreement Check (spanning tree), 105, 107
no-learning action (loop detection), 122
normal

voice VLAN mode, 177
notification
MAC address move, 29
notifying
MAC address table SNMP notification, 31
MAC Information change notification interval, 35
null interface
configuration, 16, 16
display, 17
maintain, 17

O

operational key (Ethernet link aggregation), 39
organization-specific LLDPDU TLV types, 236
OUI
voice VLAN IP phone identification (OUI address), 173
voice VLAN IP phone identification method, 173
outputting
spanning tree port state transition information, 101

P

packet
1:1 VLAN mapping configuration, 220, 226
1:2 VLAN mapping configuration, 225, 231
2:2 VLAN mapping configuration, 225, 231
Ethernet link aggregation group BFD, 52
Ethernet link aggregation packet type-based load sharing, 45
LLDP CDP compatibility, 247
M:1 VLAN mapping configuration, 220, 226
M:1 VLAN mapping configuration (dynamic IP address assignment), 221
M:1 VLAN mapping configuration (static IP address assignment), 223
service loopback group configuration, 256, 257
spanning tree port mode configuration, 100
STP BPDU protocol packets, 73
STP TCN BPDU protocol packets, 73
VLAN mapping configuration, 214, 219, 226
parameter
spanning tree timeout factor, 95
per-flow load sharing, 45, 55
performing
spanning tree mCheck, 102
per-packet load sharing, 45
Per-VLAN Spanning Tree Protocol. *Use* PVST
physical
interface physical state change suppression (Ethernet), 5
polling
interface statistics polling interval (Ethernet), 8
LLDP enable, 242
port
Ethernet aggregate interface, 49
Ethernet aggregate interface (description), 49
Ethernet aggregate interface (Layer 3 edge), 68
Ethernet link aggregate group Selected ports min/max, 50
Ethernet link aggregate interface (expected bandwidth), 51
Ethernet link aggregate interface (Layer 2 edge), 64
Ethernet link aggregate interface default settings, 53
Ethernet link aggregate interface shutdown, 53
Ethernet link aggregation (dynamic mode), 41
Ethernet link aggregation (Layer 2 dynamic), 60
Ethernet link aggregation (Layer 2 static), 58
Ethernet link aggregation (Layer 3 dynamic), 67
Ethernet link aggregation (Layer 3 static), 66
Ethernet link aggregation (static mode), 40
Ethernet link aggregation configuration, 38, 45, 58
Ethernet link aggregation configuration types, 39
Ethernet link aggregation edge aggregate interface, 45, 51
Ethernet link aggregation group, 46
Ethernet link aggregation group (dynamic), 47
Ethernet link aggregation group (Layer 2 static), 46, 47
Ethernet link aggregation group (Layer 3 dynamic), 48
Ethernet link aggregation group (Layer 3 static), 47
Ethernet link aggregation group (static), 46
Ethernet link aggregation group load sharing, 54
Ethernet link aggregation LACP, 41
Ethernet link aggregation LACP port priority, 42
Ethernet link aggregation load sharing (Layer 2), 62
Ethernet link aggregation load sharing mode, 45
Ethernet link aggregation local-first load sharing, 55
Ethernet link aggregation member port, 38
Ethernet link aggregation member port state, 38, 40, 43
Ethernet link aggregation modes, 40
Ethernet link aggregation operational key, 39
Ethernet link aggregation per-flow load sharing algorithm settings, 55

Ethernet link aggregation reference port, 42
Ethernet link aggregation reference port choice, 40
Ethernet link aggregation traffic redirection, 56
interface fiber port (Layer 2 Ethernet), 12
isolation. *See* port isolation
Layer 2 aggregate interface (ignored VLAN), 50
Layer 3 aggregate interface configuration (MTU), 50
link aggregation management VLAN+management port, 57
LLDP basic configuration, 240, 250
LLDP configuration, 234, 240, 250
LLDP disable operating mode, 239
LLDP enable, 240
LLDP frame encapsulation format, 246
LLDP frame reception, 240
LLDP frame transmission, 239
LLDP operating mode, 242
LLDP polling, 242
LLDP reinitialization delay, 242
LLDP Rx operating mode, 239
LLDP Tx operating mode, 239
LLDP TxRx operating mode, 239
loop detection configuration, 121, 123, 125
loop detection enable (port-specific), 123
loop detection interval, 122, 124
loop detection protection action configuration, 124
loop detection protection actions, 122
loop detection status auto recovery, 122
M:1 VLAN mapping customer-side port (static IP address assignment), 224
M:1 VLAN mapping network-side port (dynamic IP address assignment), 222
M:1 VLAN mapping network-side port (static IP address assignment), 224
M:1VLAN mapping customer-side port (dynamic IP address assignment), 222
MAC address learning, 20
MAC address table blackhole entry, 23
MAC address table configuration, 20, 21, 32
MAC address table entry configuration, 22
MAC address table multiport unicast entry, 23
MAC Information configuration, 34, 35
MST port roles, 84
MST port states, 84
MVRP application, 187, 190, 193
MVRP timer set, 192
QinQ implementation, 205
RSTP network convergence, 80
service loopback group configuration, 256, 257
spanning tree BPDU drop, 112
spanning tree BPDU guard, 109
spanning tree BPDU transmission rate, 95
spanning tree dispute guard, 112
spanning tree edge port configuration, 95
spanning tree forward delay timer, 93
spanning tree loop guard, 110
spanning tree path cost calculation standard, 96
spanning tree path cost configuration, 96, 98
spanning tree port link type configuration, 100
spanning tree port mode configuration, 100
spanning tree port priority configuration, 99
spanning tree port role restriction, 110
spanning tree port state transition output, 101
spanning tree root guard, 109
spanning tree TC-BPDU guard, 111
spanning tree TC-BPDU transmission restriction, 111
STP designated port, 74
STP root port, 74
VLAN port link type, 131
voice VLAN port mode, 177
voice VLAN port operation configuration (automatic assignment), 179
voice VLAN port operation configuration (manual assignment), 180
port isolation
configuration, 70, 71
display, 70
group assignment (multiple ports), 70
port-based VLAN
assignment (access port), 132
assignment (hybrid port), 133
assignment (trunk port), 133
configuration, 131, 142
port frame handling, 131
port link type, 131
PVID, 131
power
interface auto power-down (Ethernet), 7
interface EEE (Ethernet), 8
interface energy-saving features (Ethernet), 7
priority
Ethernet link aggregation LACP, 41
Ethernet link aggregation LACP port priority, 42
Ethernet link aggregation LACP system priority, 42
MAC address table learning priority, 27
QinQ SVLAN tag 802.1p priority, 208
spanning tree device priority, 92

spanning tree port priority configuration, 99
private VLAN
configuration, 156, 157, 159
configuration restrictions, 157
display, 159
promiscuous port configuration, 159
secondary VLAN Layer 3 communication configuration, 170
trunk promiscuous port configuration, 162
trunk promiscuous+secondary port configuration, 165
procedure
adding MAC address table blackhole entry, 23
adding MAC address table entry (global), 22
adding MAC address table entry (on interface), 22
adding MAC address table multiport unicast entry, 23
advertising authorization VLAN (CDP), 182
advertising authorization VLAN (LLDP), 182
assigning MAC address table learning priority to interface, 27
assigning port isolation group (multiple ports), 70
assigning port-based VLAN access port (interface view), 132
assigning port-based VLAN access port (VLAN view), 132
assigning port-based VLAN hybrid port, 133
assigning port-based VLAN trunk port, 133
bulk configuring interfaces, 18, 18
changing combo interface active port (Ethernet combo), 2
combining interfaces (Ethernet 10-GE > 40-GE), 2
configuring 1:1 VLAN mapping, 220, 226
configuring 1:2 VLAN mapping, 225, 231
configuring 2:2 VLAN mapping, 225, 231
configuring combo interface, 2
configuring Ethernet aggregate interface, 49
configuring Ethernet aggregate interface (description), 49
configuring Ethernet aggregate interface (Layer 3 edge), 68
configuring Ethernet link aggregate interface (Layer 2 edge), 64
configuring Ethernet link aggregation, 45
configuring Ethernet link aggregation (Layer 2 dynamic), 60
configuring Ethernet link aggregation (Layer 2 static), 58
configuring Ethernet link aggregation (Layer 3 dynamic), 67
configuring Ethernet link aggregation (Layer 3 static), 66
configuring Ethernet link aggregation edge aggregate interface, 51
configuring Ethernet link aggregation group, 46
configuring Ethernet link aggregation group (dynamic), 47
configuring Ethernet link aggregation group (Layer 2 dynamic), 47
configuring Ethernet link aggregation group (Layer 2 static), 46
configuring Ethernet link aggregation group (Layer 3 dynamic), 48
configuring Ethernet link aggregation group (Layer 3 static), 47
configuring Ethernet link aggregation group (static), 46
configuring Ethernet link aggregation group BFD, 52
configuring Ethernet link aggregation group load sharing, 54
configuring Ethernet link aggregation load sharing (Layer 2), 62
configuring Ethernet link aggregation per-flow load sharing algorithm settings, 55
configuring interface (inloopback), 17
configuring interface (Layer 2 Ethernet), 9
configuring interface (Layer 3 Ethernet), 14
configuring interface (loopback), 16
configuring interface (null), 16
configuring interface auto power-down (Ethernet), 7
configuring interface basic settings (Ethernet), 3
configuring interface card operating mode (Ethernet), 8
configuring interface common settings (Ethernet), 1
configuring interface EEE (Ethernet), 8
configuring interface energy-saving features (Ethernet), 7
configuring interface generic flow control (Ethernet), 6
configuring interface jumbo frame support (Ethernet), 4
configuring interface link mode (Ethernet), 4
configuring interface physical state change suppression (Ethernet), 5
configuring interface storm control (Layer 2 Ethernet), 10
configuring interface storm suppression (Ethernet), 9
configuring IP subnet-based VLAN, 139, 146
configuring LAN switching QinQ CVLAN tag TPID value, 208

configuring LAN switching QinQ SVLAN tag TPID value, 208
configuring LAN switching QinQ VLAN tag TPID value, 207
configuring LAN switching spanning tree Digest Snooping, 104
configuring LLDP, 240
configuring LLDP (CDP-compatible), 254
configuring LLDP advertisable TLVs, 243
configuring LLDP basics, 240, 250
configuring LLDP CDP compatibility, 247
configuring LLDP management address, 245
configuring LLDP management address encoding format, 245
configuring LLDP trapping, 248
configuring LLDP-MED trapping, 248
configuring loop detection, 123, 125
configuring loop detection protection action, 124
configuring loop detection protection action (global), 124
configuring loop detection protection action (Layer 2 aggregate interface), 124
configuring loop detection protection action (Layer 2 Ethernet interface), 124
configuring M:1 VLAN mapping, 220, 226
configuring M:1 VLAN mapping (dynamic IP address assignment), 221
configuring M:1 VLAN mapping (static IP address assignment), 223
configuring M:1 VLAN mapping customer-side port (dynamic IP address assignment), 222
configuring M:1 VLAN mapping customer-side port (static IP address assignment), 224
configuring M:1 VLAN mapping network-side port (dynamic IP address assignment), 222
configuring M:1 VLAN mapping network-side port (static IP address assignment), 224
configuring MAC address table, 21, 32
configuring MAC address table entry, 22
configuring MAC address table frame forwarding rule, 26
configuring MAC address table multiport unicast entry (global), 24
configuring MAC address table multiport unicast entry (on interface), 24
configuring MAC Information, 35
configuring MAC Information mode, 34
configuring MAC-based VLAN, 134, 144
configuring MAC-based VLAN (server-assigned), 138
configuring MAC-based VLAN assignment (dynamic), 138
configuring MAC-based VLAN assignment (static), 137
configuring management interface, 1
configuring MST region, 90
configuring MST region max hops, 92
configuring MSTP, 88, 114
configuring MVRP, 190, 193
configuring port-based VLAN, 131, 142
configuring private VLAN, 157
configuring private VLAN promiscuous port, 159
configuring private VLAN trunk promiscuous port, 162
configuring private VLAN trunk promiscuous+secondary port, 165
configuring protocol-based VLAN, 140, 147
configuring PVST, 88, 117
configuring QinQ, 210
configuring QinQ basics, 210
configuring QinQ VLAN transparent transmission, 206, 212
configuring RSTP, 87
configuring secondary VLAN Layer 3 communication, 170
configuring service loopback group, 256, 257
configuring spanning tree, 86, 114
configuring spanning tree BPDU transmission rate, 95
configuring spanning tree device priority, 92
configuring spanning tree Digest Snooping, 103
configuring spanning tree edge port, 95
configuring spanning tree No Agreement Check, 105, 107
configuring spanning tree port link type, 100
configuring spanning tree port mode for MSTP packets, 100
configuring spanning tree port path cost, 96, 98
configuring spanning tree port priority, 99
configuring spanning tree port role restriction, 110
configuring spanning tree protection functions, 108
configuring spanning tree root bridge, 91
configuring spanning tree root bridge (device), 91
configuring spanning tree secondary root bridge, 91
configuring spanning tree secondary root bridge (device), 91
configuring spanning tree switched network diameter, 93
configuring spanning tree TC Snooping, 107
configuring spanning tree TC-BPDU transmission restriction, 111
configuring spanning tree timeout factor, 95

configuring spanning tree timer, 93
configuring STP, 87
configuring super VLAN, 151, 151, 153
configuring super VLAN interface, 152
configuring VLAN basic settings, 129
configuring VLAN group, 141
configuring VLAN interface, 130
configuring VLAN mapping, 219
configuring voice VLAN, 175
configuring voice VLAN advertisement (CDP), 181
configuring voice VLAN advertisement (LLDP), 181
configuring voice VLAN assignment mode (automatic), 183
configuring voice VLAN assignment mode (manual), 185
configuring voice VLAN port operation (automatic assignment), 179
configuring voice VLAN port operation (manual assignment), 180
configuring voice VLAN traffic QoS priority settings, 178
creating super VLAN sub-VLAN, 151
disabling MAC address learning, 24
disabling MAC address learning (global), 24
disabling MAC address learning (on interface), 25
disabling MAC address learning (on VLAN), 25
displaying bulk interface configuration, 19
displaying Ethernet link aggregation, 58
displaying interface, 17
displaying interface (Ethernet), 15
displaying LLDP, 249
displaying loop detection, 125
displaying MAC address table, 31
displaying MVRP, 193
displaying port isolation, 70
displaying private VLAN, 159
displaying QinQ, 209
displaying service loopback group, 256
displaying spanning tree, 113
displaying super VLAN, 152
displaying VLAN, 142
displaying VLAN mapping, 226
displaying voice VLAN, 183
enable interface bridging (Layer 2 Ethernet), 14
enabling Ethernet link aggregation local-first load sharing, 55
enabling Ethernet link aggregation traffic redirection, 56
enabling interface automatic negotiation (Ethernet), 9
enabling interface loopback testing (Ethernet), 6
enabling LLDP, 240
enabling LLDP polling, 242
enabling loop detection (global), 123
enabling loop detection (port-specific), 123
enabling M:1 VLAN mapping ARP detection (dynamic IP address assignment), 221
enabling M:1 VLAN mapping ARP snooping (static IP address assignment), 223
enabling M:1 VLAN mapping DHCP snooping (dynamic IP address assignment), 221
enabling MAC address move notification, 29
enabling MAC address synchronization, 28
enabling MAC address table ARP fast update, 30
enabling MAC address table SNMP notification, 31
enabling MAC Information, 34
enabling MVRP, 191
enabling MVRP GVRP compatibility, 193
enabling QinQ, 206
enabling spanning tree BPDU drop, 112
enabling spanning tree BPDU guard, 109
enabling spanning tree dispute guard, 112
enabling spanning tree feature, 101
enabling spanning tree loop guard, 110
enabling spanning tree port state transition information output, 101
enabling spanning tree root guard, 109
enabling spanning tree TC-BPDU guard, 111
enabling voice VLAN LLDP automatic IP phone discovery, 181
forcing interface fiber port (Layer 2 Ethernet), 12
maintaining Ethernet link aggregation, 58
maintaining interface, 17
maintaining interface (Ethernet), 15
maintaining MVRP, 193
maintaining spanning tree, 113
maintaining VLAN, 142
modifying MAC address table blackhole entry, 23
modifying MAC address table entry (global), 22
modifying MAC address table entry (on interface), 22
modifying MAC address table multiport unicast entry, 23
performing spanning tree mCheck, 102
restoring Ethernet link aggregate interface default settings, 53

setting Ethernet link aggregate group Selected ports min/max, 50
setting Ethernet link aggregate interface (expected bandwidth), 51
setting Ethernet link aggregation load sharing mode (global), 54
setting Ethernet link aggregation load sharing mode (group-specific), 54
setting interface MDIX mode (Layer 2 Ethernet), 13
setting interface MTU (Layer 3 Ethernet), 14
setting interface statistics polling interval (Ethernet), 8
setting Layer 3 aggregate interface (MTU), 50
setting LLDP frame encapsulation format, 246
setting LLDP operating mode, 242
setting LLDP parameters, 246
setting LLDP reinitialization delay, 242
setting loop detection interval, 124
setting MAC address table dynamic aging timer, 25
setting MAC address table learning limit, 26
setting MAC Information change notification interval, 35
setting MAC Information queue length, 35
setting MVRP registration mode, 192
setting MVRP timer, 192
setting QinQ SVLAN tag 802.1p priority, 208
setting spanning tree mode, 89
shutting down Ethernet link aggregate interface, 53
specifying Layer 2 aggregate interface (ignored VLAN), 50
specifying link aggregation management VLAN+management port, 57, 57
specifying spanning tree port path cost calculation standard, 96
splitting interface (Ethernet 40-GE), 2
testing interface cable connection (Layer 2 Ethernet), 14
promiscuous
private VLAN promiscuous port configuration, 159
private VLAN trunk promiscuous port configuration, 162
private VLAN trunk promiscuous+secondary port configuration, 165
protecting
loop detection protection action configuration, 124
spanning tree protection functions, 108
protocol-based VLAN
configuration, 140, 147
protocols and standards
Ethernet link aggregation protocol configuration, 39
LLDP, 240
MSTP, 86
MVRP, 190
QinQ, 205
STP protocol packets, 73
VLAN, 129
PVID (port-based VLAN), 131
PVST, 73, *See also* STP
configuration, 88, 117
feature enable, 102
mode set, 89
port links, 80

Q

QinQ
basic configuration, 210
configuration, 204, 210
configuration restrictions, 206
CVLAN tag, 204
CVLAN tag TPID value, 208
display, 209
enable, 206
how it works, 204
implementation, 205
loop detection configuration, 121, 123, 125
protocols and standards, 205
SVLAN tag, 204
SVLAN tag 802.1p priority, 208
SVLAN tag TPID value, 208
VLAN tag TPID value, 207
VLAN transparent transmission, 206
VLAN transparent transmission configuration, 212
QoS
QinQ SVLAN tag 802.1p priority, 208
voice VLAN traffic QoS priority settings, 178
queuing
MAC Information queue length, 35

R

Rapid Spanning Tree Protocol. *Use* RSTP
rate
spanning tree BPDU transmission rate, 95
receiving
LLDP frames, 240
recovering
loop detection port status auto recovery, 122
redirecting

Ethernet link aggregation traffic redirection, 56
reference port (Ethernet link aggregation), 40, 42
region
MST, 82
MST region configuration, 90
MST region max hops, 92
MST regional root, 83
registering
MVRP registration fixed mode, 190
MVRP registration forbidden mode, 190
MVRP registration mode, 192
MVRP registration normal mode, 190
reinitialization delay (LLDP), 242
restoring
Ethernet link aggregate interface default settings, 53
restrictions
bulk interface configuration, 18
Ethernet link aggregation BFD configuration, 52
Ethernet link aggregation group, 46
Ethernet link aggregation traffic redirection, 56
interface dampening (Ethernet), 6
LAN switching STP Digest Snooping configuration, 104
LAN switching STP edge port configuration, 96
LAN switching STP mCheck configuration, 103
LAN switching STP port link type configuration, 100
LAN switching STP TC Snooping configuration, 108
LAN switching STP timer configuration, 94
Layer 2 Ethernet interface fiber port, 12
M:1 VLAN mapping configuration (dynamic IP address assignment), 221
M:1 VLAN mapping configuration (static IP address assignment), 223
MAC Information configuration, 36
MAC-based VLAN assignment configuration (dynamic), 180
MVRP configuration, 190
private VLAN configuration, 157
QinQ configuration, 206
spanning tree port role restriction, 110
spanning tree TC-BPDU transmission restriction, 111
VLAN interface resource reservation, 179
voice VLAN port operation configuration (automatic assignment), 137
voice VLAN port operation configuration restrictions (manual assignment), 181
root
MST common root bridge, 83
MST regional root, 83
MST root port role, 84
spanning tree root bridge, 91
spanning tree root bridge (device), 91
spanning tree root guard, 109
spanning tree secondary root bridge (device), 91
STP algorithm calculation, 74
STP root bridge, 73
STP root port, 74
routing
IP subnet-based VLAN configuration, 139, 146
MAC-based VLAN assignment (dynamic), 138
MAC-based VLAN assignment (static), 137
MAC-based VLAN configuration, 134, 144
MAC-based VLAN configuration (server-assigned), 138
protocol-based VLAN configuration, 140, 147
voice VLAN configuration, 173, 175, 183
voice VLAN IP phone access method, 175
RSTP, 73, *See also* STP
configuration, 87
feature enable, 102
mode set, 89
MSTP device implementation, 85
network convergence, 80
rule
MAC address table frame forwarding, 26

S

security
voice VLAN mode, 177
selecting
Ethernet link aggregation Selected ports min/max, 50
Ethernet link aggregation selected state, 38
Ethernet link aggregation unselected state, 38
series
voice VLAN host+IP phone connection (in series), 175
server
MAC-based VLAN assignment (server-assigned), 136
MAC-based VLAN configuration (server-assigned), 138
service loopback group
configuration, 256, 257
display, 256
setting

Ethernet link aggregate group Selected ports min/max, 50
Ethernet link aggregate interface (expected bandwidth), 51
Ethernet link aggregation load sharing mode (global), 54
Ethernet link aggregation load sharing mode (group-specific), 54
Ethernet link aggregation member port state, 40, 43
interface MDIX mode (Layer 2 Ethernet), 13
interface statistics polling interval (Ethernet), 8
Layer 3 aggregate interface (MTU), 50
LLDP frame encapsulation format, 246
LLDP operating mode, 242
LLDP parameters, 246
LLDP reinitialization delay, 242
loop detection interval, 124
MAC address table dynamic aging timer, 25
MAC address table learning limit, 26
MAC Information change notification interval, 35
MAC Information queue length, 35
MVRP registration mode, 192
MVRP timer, 192
QinQ SVLAN tag 802.1p priority, 208
spanning tree mode, 89
shutting down
Ethernet link aggregate interface, 53
loop detection shutdown action, 122
SNAP
LLDP frame encapsulation, 235
LLDP frame encapsulation format, 246
SNMP
MAC address table SNMP notification, 31
MAC Information configuration, 34, 35
snooping
spanning tree Digest Snooping, 103, 104
spanning tree TC Snooping, 107
spanning tree, 73, *See also STP, RSTP, PVST, MSTP*
BPDU drop, 112
BPDU guard enable, 109
BPDU transmission rate configuration, 95
configuration, 73, 86, 114
device priority configuration, 92
Digest Snooping, 103, 104
displaying, 113
dispute guard enable, 112
edge port configuration, 95
feature enable, 101
loop guard enable, 110
maintaining, 113
mCheck, 102
mode set, 89
MST region max hops, 92
MSTP, 80, *See also* MSTP
No Agreement Check, 105, 107
port link type configuration, 100
port mode configuration, 100
port path cost calculation standard, 96
port path cost configuration, 96, 98
port priority configuration, 99
port role restriction, 110
port state transition output, 101
protection functions, 108
PVST, 80, *See also* PVST
root bridge configuration, 91
root bridge configuration (device), 91
root guard enable, 109
RSTP, 80, *See also* RSTP
secondary root bridge configuration (device), 91
switched network diameter, 93
TC Snooping, 107
TC-BPDU guard, 111
TC-BPDU transmission restriction, 111
timeout factor configuration, 95
timer configuration, 93
specifying
Layer 2 aggregate interface (ignored VLAN), 50
link aggregation management VLAN+management port, 57
spanning tree port path cost calculation standard, 96
splitting
interface (Ethernet 40-GE), 2
state
Ethernet link aggregation member port state, 38, 40, 43
interface state change suppression (Ethernet), 5
static
Ethernet link aggregation (Layer 2), 58
Ethernet link aggregation (Layer 3), 66
Ethernet link aggregation (static mode), 40
Ethernet link aggregation group, 46
Ethernet link aggregation group BFD, 52
Ethernet link aggregation mode, 40
Layer 2 Ethernet link aggregation group, 46
Layer 3 Ethernet link aggregation group, 47
MAC address table entry, 20
MAC address table entry configuration (global), 22

MAC address table entry configuration (on interface), 22
MAC-based VLAN assignment, 134, 137
statistics
interface automatic negotiation (Ethernet), 9
interface statistics polling interval (Ethernet), 8
storm
interface storm control (Layer 2 Ethernet), 10
interface storm suppression (Ethernet), 9
STP
algorithm calculation, 74
basic concepts, 73
BPDU forwarding, 79
configuration, 87
designated bridge, 74
designated port, 74
Digest Snooping configuration restrictions, 104
edge port configuration restrictions, 96
feature enable, 102
loop detection, 73
mCheck configuration restrictions, 103
mode set, 89
MSTP device implementation, 85
path cost, 74
port link type configuration restrictions, 100
protocol packets, 73
root bridge, 73
root port, 74
TC Snooping configuration restrictions, 108
timer configuration restrictions, 94
timers, 79
subinterface, 1, *See also* Ethernet subinterface
subnetting
IP subnet-based VLAN configuration, 139, 146
sub-VLAN
creation, 151
super VLAN
configuration, 151, 151, 153
display, 152
interface configuration, 152
sub-VLAN creation, 151
suppressing
interface physical state change suppression (Ethernet), 5
interface storm control configuration (Layer 2 Ethernet), 10
interface storm suppression (Ethernet), 9
SVLAN
QinQ basic configuration, 210
QinQ configuration, 204, 210
QinQ SVLAN tag 802.1p priority, 208
QinQ VLAN transparent transmission configuration, 212
VLAN mapping configuration, 214, 219, 226
VLAN mapping implementation, 216
switching
interface configuration (Ethernet), 1
interface configuration (inloopback), 16, 17
interface configuration (loopback), 16, 16
interface configuration (null), 16, 16
spanning tree switched network diameter, 93
synchronizing
MAC addresses, 28
syslog
MAC Information configuration, 34, 35
MAC Information mode configuration, 34
system
interface bulk configuration, 18, 18

T

table
MAC address, 20, 21, 32
MAC address table learning limit, 26
MSTP VLAN-to-instance mapping table, 83
tag
1:1 VLAN mapping configuration, 220, 226
1:2 VLAN mapping configuration, 225, 231
2:2 VLAN mapping configuration, 225, 231
M:1 VLAN mapping configuration, 220, 226
M:1 VLAN mapping configuration (dynamic IP address assignment), 221
M:1 VLAN mapping configuration (static IP address assignment), 223
QinQ CVLAN, 204
QinQ CVLAN tag TPID value, 208
QinQ SVLAN, 204
QinQ SVLAN tag 802.1p priority, 208
QinQ SVLAN tag TPID value, 208
QinQ VLAN tag TPID value, 207
VLAN mapping configuration, 214, 219, 226
TC Snooping (spanning tree), 107
TC-BPDU
spanning tree TC-BPDU guard, 111
spanning tree TC-BPDU transmission restriction, 111
testing
interface cable connection (Layer 2 Ethernet), 14
time
Ethernet link aggregation LACP timeout interval, 41

timeout
Ethernet link aggregation LACP long timeout interval, 42
Ethernet link aggregation LACP short timeout interval, 42
spanning tree timeout factor, 95
timer
LLDP reinitialization delay, 242
MAC address table dynamic aging, 25
MRP Join, 189
MRP Leave, 189
MRP LeaveAll, 189
MRP Periodic, 189
MVRP set, 192
spanning tree forward delay, 93
spanning tree hello, 93
spanning tree max age, 93
STP forward delay, 79
STP hello, 79
STP max age, 79
TLV
LLDP advertisable TLV configuration, 243
LLDP management address configuration, 245
LLDP management address encoding format, 245
LLDP parameters, 246
LLDPDU basic management types, 236
LLDPDU LLDP-MED types, 236
LLDPDU management address TLV, 239
LLDPDU organization-specific types, 236
topology
STP TCN BPDU protocol packets, 73
traffic
Ethernet link aggregation traffic redirection, 56
private VLAN configuration, 157, 159
voice VLAN traffic QoS priority settings, 178
transmitting
LLDP frames, 239
QinQ VLAN transparent transmission, 206, 212
spanning tree TC-BPDU transmission restriction, 111
transparent transmission (QinQ for VLAN), 206, 212
trapping
LLDP configuration, 248
LLDP-MED configuration, 248
MAC address table SNMP notification, 31
MAC Information configuration, 34, 35
MAC Information mode configuration, 34
trunk port
port-based VLAN assignment (trunk port), 133
private VLAN trunk promiscuous port configuration, 162
private VLAN trunk promiscuous+secondary port configuration, 165

U

unicast
MAC address table configuration, 20, 21, 32
MAC address table multiport unicast entry, 20

V

virtual
Virtual Local Area Network. *Use* VLAN
VLAN
authorization VLAN advertisement (CDP), 182
authorization VLAN advertisement (LLDP), 182
basic configuration, 129
configuration, 128, 142
display, 142
frame encapsulation, 128
group configuration, 141
interface configuration, 130
interface resource reservation restrictions, 179
IP subnet-based VLAN configuration, 139, 146
Layer 2 Ethernet aggregate interface (ignored VLAN), 50
link aggregation management VLAN+management port, 57
LLDP CDP compatibility, 247
LLDP configuration (CDP-compatible), 254
loop detection configuration, 121, 123, 125
MAC address learning disable, 25
MAC-based assignment (dynamic), 138
MAC-based assignment (static), 137
MAC-based configuration, 144
MAC-based VLAN configuration, 134
MAC-based VLAN configuration (server-assigned), 138
maintain, 142
mapping. *See* VLAN mapping
MRP implementation, 187
MSTP VLAN-to-instance mapping table, 83
MVRP configuration, 187, 190, 193
MVRP GVRP compatibility, 193
port isolation configuration, 70, 71
port link type, 131
port-based configuration, 131, 142
port-based VLAN assignment (access port), 132
port-based VLAN assignment (hybrid port), 133
port-based VLAN assignment (trunk port), 133

port-based VLAN frame handling, 131
private VLAN configuration, 156, 157
private VLAN configuration restrictions, 157
protocol-based VLAN configuration, 140, 147
protocols and standards, 129
PVID, 131
PVST, 80
QinQ basic configuration, 210
QinQ configuration, 204, 210
QinQ CVLAN tag, 204
QinQ CVLAN tag TPID value, 208
QinQ implementation, 205
QinQ SVLAN tag, 204
QinQ SVLAN tag 802.1p priority, 208
QinQ SVLAN tag TPID value, 208
QinQ transparent transmission, 206
QinQ VLAN tag TPID value, 207
QinQ VLAN transparent transmission configuration, 212
super VLAN configuration, 151, 151, 153
super VLAN interface configuration, 152
voice VLAN advertisement (CDP), 181
voice VLAN advertisement (LLDP), 181
voice VLAN assignment mode, 175
voice VLAN assignment mode configuration (automatic), 183
voice VLAN assignment mode configuration (manual), 185
voice VLAN configuration, 173, 175, 183
voice VLAN host+IP phone connection (in series), 175
voice VLAN IP phone access method, 175
voice VLAN IP phone+device connection, 175
voice VLAN LLDP automatic IP phone discovery enable, 181
voice VLAN port mode, 177
voice VLAN port operation configuration (automatic assignment), 179
voice VLAN port operation configuration (manual assignment), 180
voice VLAN port operation configuration restrictions (automatic assignment), 137
voice VLAN port operation configuration restrictions (manual assignment), 181
voice VLAN traffic QoS priority settings, 178
VLAN mapping
1:1 application scenario, 214
1:1 configuration, 220, 226
1:1 implementation, 216, 217
1:2 application scenario, 216
1:2 configuration, 225, 231
1:2 implementation, 216, 218
2:2 application scenario, 216
2:2 configuration, 225, 231
2:2 implementation, 216, 218
configuration, 214, 219, 226
display, 226
M:1 application scenario, 214
M:1 configuration, 220, 226
M:1 configuration (dynamic IP address assignment), 221
M:1 configuration (static IP address assignment), 223
M:1 implementation, 216, 217
voice traffic
LLDP CDP compatibility, 247
LLDP configuration (CDP-compatible), 254
voice VLAN
advertisement configuration (CDP), 181
advertisement configuration (LLDP), 181
assignment mode, 175
assignment mode (automatic), 175
assignment mode (manual), 176
assignment mode configuration (automatic), 183
assignment mode configuration (manual), 185
assignment mode+IP phone cooperation, 176
configuration, 173, 175, 183
display, 183
host+IP phone connection (in series), 175
information advertisement to IP phone, 174
IP phone access method, 175
IP phone identification (LLDP), 174
IP phone identification (OUI address), 173
IP phone identification method, 173
IP phone+device connection, 175
LLDP automatic IP phone discovery enable, 181
port mode, 177
port operation configuration (automatic assignment), 179
port operation configuration (manual assignment), 180
port operation configuration restrictions (automatic assignment), 137
port operation configuration restrictions (manual assignment), 181
traffic QoS priority setting configuration, 178
VoIP
voice VLAN configuration, 173, 175, 183
voice VLAN information advertisement to IP phones, 174
voice VLAN IP phone access method, 175
voice VLAN IP phone identification (LLDP), 174

voice VLAN IP phone identification (OUI address), 173
VPN
QinQ basic configuration, 210
QinQ configuration, 204, 210
QinQ VLAN transparent transmission configuration, 212