



Hewlett Packard
Enterprise

HPE FlexNetwork 5130 EI Switch Series

Layer 2—LAN Switching Configuration Guide

Part number: 5998-5481s
Software version: Release 3111P02 and later
Document version: 6W101-20161010

© Copyright 2015, 2016 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 trademarks of the Microsoft group of companies.

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
Ethernet interface naming conventions	1
Configuring common Ethernet interface settings	1
Configuring a combo interface	1
Configuring basic settings of an Ethernet interface	2
Configuring jumbo frame support	2
Configuring physical state change suppression on an Ethernet interface	3
Performing a loopback test on an Ethernet interface	4
Configuring generic flow control on an Ethernet interface	4
Enabling energy saving functions on an Ethernet interface	5
Setting the statistics polling interval	6
Configuring storm suppression	6
Configuring storm control on an Ethernet interface	7
Forcibly bringing up a fiber port	8
Setting the MDIX mode of an Ethernet interface	10
Testing the cable connection of an Ethernet interface	10
Enabling bridging on an Ethernet interface	11
Configuring speed downgrade autonegotiation	11
Displaying and maintaining an Ethernet interface	12
Configuring loopback, null, and inloopback interfaces	13
Configuring a loopback interface	13
Configuring a null interface	13
Configuring an inloopback interface	14
Displaying and maintaining loopback, null, and inloopback interfaces	14
Bulk configuring interfaces	15
Configuration restrictions and guidelines	15
Configuration procedure	15
Displaying and maintaining bulk interface configuration	16
Configuring the MAC address table	17
Overview	17
How a MAC address entry is created	17
Types of MAC address entries	17
Configuring the MAC address table configuration task list	18
Configuring MAC address entries	19
Configuration guidelines	19
Adding or modifying a static or dynamic MAC address entry globally	19
Adding or modifying a static or dynamic MAC address entry on an interface	19
Adding or modifying a blackhole MAC address entry	20
Adding or modifying a multiport unicast MAC address entry	20
Disabling MAC address learning	21
Disabling global MAC address learning	21
Disabling MAC address learning on an interface	22
Disabling MAC address learning on a VLAN	22
Configuring the aging timer for dynamic MAC address entries	22
Configuring the MAC learning limit on an interface	23
Configuring the device to forward unknown frames after the MAC learning limit on an interface is reached ..	23
Enabling MAC address synchronization	24
Enable MAC address move notifications	25
Enabling ARP fast update for MAC address moves	26
Disabling static source check	27
Enabling SNMP notifications for the MAC address table	28
Displaying and maintaining the MAC address table	28
MAC address table configuration example	28
Network requirements	28

Configuration procedure.....	29
Verifying the configuration.....	29
Configuring MAC Information.....	30
Enabling MAC Information.....	30
Configuring the MAC Information mode.....	30
Configuring the MAC change notification interval.....	31
Configuring the MAC Information queue length.....	31
MAC Information configuration example.....	31
Network requirements.....	31
Configuration restrictions and guidelines.....	32
Configuration procedure.....	32
Configuring Ethernet link aggregation.....	34
Basic concepts.....	34
Aggregation group, member port, and aggregate interface.....	34
Aggregation states of member ports in an aggregation group.....	34
Operational key.....	34
Configuration types.....	35
Link aggregation modes.....	35
Aggregating links in static mode.....	36
Choosing a reference port.....	36
Setting the aggregation state of each member port.....	36
Aggregating links in dynamic mode.....	37
LACP.....	37
How dynamic link aggregation works.....	38
Load sharing modes for link aggregation groups.....	40
Ethernet link aggregation configuration task list.....	40
Configuring an aggregation group.....	41
Configuration restrictions and guidelines.....	41
Configuring a static aggregation group.....	41
Configuring a dynamic aggregation group.....	42
Configuring an aggregate interface.....	42
Configuring the description of an aggregate interface.....	42
Specifying ignored VLANs for a Layer 2 aggregate interface.....	43
Setting the minimum and maximum numbers of Selected ports for an aggregation group.....	43
Setting the expected bandwidth of an aggregate interface.....	44
Enabling BFD for an aggregation group.....	44
Shutting down an aggregate interface.....	45
Restoring the default settings for an aggregate interface.....	45
Configuring load sharing for link aggregation groups.....	46
Setting load sharing modes for link aggregation groups.....	46
Enabling local-first load sharing for link aggregation.....	46
Enabling link-aggregation traffic redirection.....	47
Configuration restrictions and guidelines.....	47
Configuration procedure.....	48
Displaying and maintaining Ethernet link aggregation.....	48
Ethernet link aggregation configuration examples.....	48
Layer 2 static aggregation configuration example.....	48
Layer 2 dynamic aggregation configuration example.....	50
Layer 2 aggregation load sharing configuration example.....	52
Configuring port isolation.....	55
Assigning a port to an isolation group.....	55
Displaying and maintaining port isolation.....	55
Port isolation configuration example.....	56
Network requirements.....	56
Configuration procedure.....	56
Verifying the configuration.....	56
Configuring spanning tree protocols.....	58
STP.....	58

STP protocol packets	58
Basic concepts in STP	59
Calculation process of the STP algorithm	60
RSTP	65
PVST	66
MSTP	66
MSTP features	66
MSTP basic concepts	66
How MSTP works	70
MSTP implementation on devices	71
Protocols and standards	71
Spanning tree configuration task lists	71
STP configuration task list	72
RSTP configuration task list	72
PVST configuration task list	73
MSTP configuration task list	74
Setting the spanning tree mode	74
Configuration restrictions and guidelines	75
Configuration procedure	75
Configuring an MST region	75
Configuring the root bridge or a secondary root bridge	76
Configuring the current device as the root bridge of a specific spanning tree	77
Configuring the current device as a secondary root bridge of a specific spanning tree	77
Configuring the device priority	77
Configuring the maximum hops of an MST region	78
Configuring the network diameter of a switched network	78
Setting spanning tree timers	79
Configuration restrictions and guidelines	79
Configuration procedure	79
Setting the timeout factor	80
Configuring the BPDUs transmission rate	80
Configuring edge ports	81
Configuration restrictions and guidelines	81
Configuration procedure	81
Configuring path costs of ports	81
Specifying a standard for the device to use when it calculates the default path cost	82
Configuring path costs of ports	84
Configuration example	84
Configuring the port priority	85
Configuring the port link type	85
Configuration restrictions and guidelines	85
Configuration procedure	86
Configuring the mode a port uses to recognize and send MSTP packets	86
Enabling outputting port state transition information	87
Enabling the spanning tree feature	87
Enabling the spanning tree feature in STP/RSTP/MSTP mode	87
Enabling the spanning tree feature in PVST mode	88
Performing mCheck	88
Configuration restrictions and guidelines	88
Configuration procedure	88
Configuring Digest Snooping	89
Configuration restrictions and guidelines	89
Configuration procedure	90
Digest Snooping configuration example	90
Configuring No Agreement Check	91
Configuration prerequisites	92
Configuration procedure	92
No Agreement Check configuration example	93
Configuring TC Snooping	93
Configuration restrictions and guidelines	94
Configuration procedure	94
Configuring protection functions	94

Enabling BPDU guard	95
Enabling root guard	95
Enabling loop guard	96
Configuring port role restriction	96
Configuring TC-BPDU transmission restriction	97
Enabling TC-BPDU guard	97
Enabling BPDU drop	98
Enabling SNMP notifications for new-root election and topology change events	98
Displaying and maintaining the spanning tree	99
Spanning tree configuration example	100
MSTP configuration example	100
PVST configuration example	103
Configuring L2PT	107
Overview	107
Background	107
L2PT operating mechanism	108
L2PT configuration task list	109
Enabling L2PT	109
Restrictions and guidelines	109
Enabling L2PT for a protocol	109
Setting the destination multicast MAC address for tunneled packets	110
Displaying and maintaining L2PT	110
L2PT configuration examples	111
Configuring L2PT for STP	111
Configuring L2PT for LACP	112
Configuring loop detection	116
Overview	116
Loop detection mechanism	116
Loop detection interval	117
Loop protection actions	117
Port status auto recovery	117
Loop detection configuration task list	118
Enabling loop detection	118
Enabling loop detection globally	118
Enabling loop detection on a port	118
Configuring the loop protection action	119
Configuring the global loop protection action	119
Configuring the loop protection action on a Layer 2 Ethernet interface	119
Configuring the loop protection action on a Layer 2 aggregate interface	119
Setting the loop detection interval	119
Displaying and maintaining loop detection	120
Loop detection configuration example	120
Network requirements	120
Configuration procedure	120
Verifying the configuration	121
Configuring VLANs	123
Overview	123
VLAN frame encapsulation	123
Protocols and standards	124
Configuring basic VLAN settings	124
Configuring basic settings of a VLAN interface	125
Configuring port-based VLANs	126
Introduction	126
Assigning an access port to a VLAN	127
Assigning a trunk port to a VLAN	128
Assigning a hybrid port to a VLAN	128
Configuring MAC-based VLANs	129
Introduction	129
Configuration restrictions and guidelines	132

Configuring static MAC-based VLAN assignment	132
Configuring dynamic MAC-based VLAN assignment	133
Configuring server-assigned MAC-based VLAN	133
Configuring IP subnet-based VLANs	134
Introduction	134
Configuration procedure	134
Configuring protocol-based VLANs	135
Introduction	135
Configuration procedure	135
Configuring a VLAN group	136
Displaying and maintaining VLANs	137
VLAN configuration examples	137
Port-based VLAN configuration example	137
MAC-based VLAN configuration example	139
IP subnet-based VLAN configuration example	141
Protocol-based VLAN configuration example	142
Configuring super VLANs	146
Super VLAN configuration task list	146
Creating a sub VLAN	146
Configuring a super VLAN	146
Configuring a super VLAN interface	147
Displaying and maintaining super VLANs	147
Super VLAN configuration example	148
Network requirements	148
Configuration procedure	148
Verifying the configuration	149
Configuring the private VLAN	151
Configuration task list	151
Configuration restrictions and guidelines	152
Configuration procedure	152
Displaying and maintaining the private VLAN	154
Private VLAN configuration examples	154
Promiscuous port configuration example	154
Trunk promiscuous port configuration example	157
Trunk promiscuous and trunk secondary port configuration example	160
Secondary VLAN Layer 3 communication configuration example	165
Configuring voice VLANs	168
Overview	168
Methods of identifying IP phones	168
Identifying IP phones through OUI addresses	168
Automatically identifying IP phones through LLDP	169
Advertising the voice VLAN information to IP phones	169
IP phone access methods	170
Connecting the host and the IP phone in series	170
Connecting the IP phone to the device	170
Configuring a voice VLAN on a port	170
Voice VLAN assignment modes	170
Security mode and normal mode of voice VLANs	172
Configuration prerequisites	173
Configuring the QoS priority settings for voice traffic	173
Configuring a port to operate in automatic mode	174
Configuring a port to operate in manual mode	175
Enabling LLDP for automatic IP phone discovery	175
Configuration prerequisites	176
Configuration restrictions and guidelines	176
Configuration procedure	176
Configuring LLDP or CDP to advertise a voice VLAN	176
Dynamically advertising an authorization VLAN through LLDP or CDP	177
Displaying and maintaining voice VLANs	177

Voice VLAN configuration examples.....	178
Automatic voice VLAN assignment mode configuration example.....	178
Manual voice VLAN assignment mode configuration example.....	180
Configuring MVRP	182
MRP.....	182
MRP implementation.....	182
MRP messages.....	182
MRP timers.....	184
MVRP registration modes.....	184
Protocols and standards.....	185
MVRP configuration task list.....	185
Configuration restrictions and guidelines.....	185
Configuration prerequisites.....	185
Enabling MVRP.....	186
Configuring an MVRP registration mode.....	186
Configuring MRP timers.....	187
Enabling GVRP compatibility.....	187
Displaying and maintaining MVRP.....	188
MVRP configuration example.....	188
Network requirements.....	188
Configuration procedure.....	189
Verifying the configuration.....	192
Configuring QinQ	198
Overview.....	198
How QinQ works.....	198
QinQ implementations.....	199
Protocols and standards.....	199
Restrictions and guidelines.....	200
Enabling QinQ.....	200
Configuring transparent transmission for VLANs.....	200
Configuring the TPID in VLAN tags.....	201
Configuring the CVLAN TPID.....	202
Configuring the SVLAN TPID.....	202
Setting the 802.1p priority in SVLAN tags.....	202
Displaying and maintaining QinQ.....	203
QinQ configuration examples.....	204
Basic QinQ configuration example.....	204
VLAN transparent transmission configuration example.....	206
Configuring VLAN mapping	208
Overview.....	208
Application scenario of one-to-one and many-to-one VLAN mapping.....	208
Application scenario of one-to-two and two-to-two VLAN mapping.....	210
VLAN mapping implementations.....	210
General configuration restrictions and guidelines.....	213
VLAN mapping configuration task list.....	213
Configuring one-to-one VLAN mapping.....	214
Configuring many-to-one VLAN mapping.....	214
Configuring many-to-one VLAN mapping in a network with dynamic IP address assignment.....	215
Configuring many-to-one VLAN mapping in a network with static IP address assignment.....	217
Configuring one-to-two VLAN mapping.....	218
Configuring two-to-two VLAN mapping.....	219
Displaying and maintaining VLAN mapping.....	220
VLAN mapping configuration examples.....	220
One-to-one and many-to-one VLAN mapping configuration example.....	220
One-to-two and two-to-two VLAN mapping configuration example.....	224
Configuring LLDP.....	228
Overview.....	228
Basic concepts.....	228

Working mechanism	233
Protocols and standards	234
LLDP configuration task list	234
Performing basic LLDP configurations	234
Enabling LLDP	234
Configuring the LLDP bridge mode	235
Setting the LLDP operating mode	235
Setting the LLDP reinitialization delay	236
Enabling LLDP polling	236
Configuring the advertisable TLVs	237
Configuring the management address and its encoding format	238
Setting other LLDP parameters	239
Setting an encapsulation format for LLDP frames	239
Disabling PVID inconsistency check	240
Configuring CDP compatibility	240
Configuration prerequisites	241
Configuration procedure	241
Configuring LLDP trapping and LLDP-MED trapping	242
Displaying and maintaining LLDP	242
LLDP configuration examples	243
Basic LLDP configuration example	243
CDP-compatible LLDP configuration example	247
Document conventions and icons	250
Conventions	250
Network topology icons	251
Support and other resources	252
Accessing Hewlett Packard Enterprise Support	252
Accessing updates	252
Websites	253
Customer self repair	253
Remote support	253
Documentation feedback	253
Index	255

Configuring Ethernet interfaces

ⓘ IMPORTANT:

When you configure the device in the BootWare menu, the last four Ethernet interfaces of the device are invisible.

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.
- **C**—Port index.

Configuring common Ethernet interface settings

Configuring a combo interface

ⓘ IMPORTANT:

This feature is applicable only to HPE FlexNetwork 5130 24G SFP 4SFP+ EI Switches (JG933A).

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
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Activate the copper combo port or fiber	combo enable { copper fiber }	By default, the copper combo

Step	Command	Remarks
combo port.		port is active.

Configuring basic settings of an Ethernet interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the interface description.	description <i>text</i>	The default setting is in the format of <i>interface-name</i> Interface . For example, GigabitEthernet1/0/1 Interface .
4. Set the duplex mode of the Ethernet interface.	duplex { auto full }	The default setting is auto for Ethernet interfaces.
5. Set the port speed.	speed { 10 100 1000 10000 auto }	The default setting is auto for Ethernet interfaces. Support for the keywords depends on the interface type. For more information, see <i>Layer 2—LAN Switching Command Reference</i> .
6. Configure the expected bandwidth of the interface.	bandwidth <i>bandwidth-value</i>	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 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 tasks:
 - 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 <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
3. Configure jumbo frame support.	jumboframe enable [<i>value</i>]	By default, the switch allows jumbo frames within 9216 bytes to pass through all Ethernet interfaces.

Configuring physical state change suppression on an Ethernet interface

ⓘ IMPORTANT:

Do not configure physical state change suppression on an Ethernet interface that has spanning tree protocols 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 tasks::

- 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
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure physical state change suppression on the interface.	link-delay [<i>msec</i>] <i>delay-time</i> [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 <i>interface-type</i> <i>interface-number</i>	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

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

Step	Command	Remarks
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable generic flow control.	<ul style="list-style-type: none"> 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 functions 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 function 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 <i>interface-type</i> <i>interface-number</i>	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 function, 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

Step	Command	Remarks
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the statistics polling interval.	flow-interval <i>interval</i>	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 storm suppression

You can use the storm suppression function 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable broadcast suppression and set the broadcast suppression threshold.	broadcast-suppression { <i>ratio</i> pps <i>max-pps</i> kbps <i>max-kbps</i> }	By default, broadcast traffic is allowed to pass through an interface.
4. Enable multicast suppression and set the multicast suppression threshold.	multicast-suppression { <i>ratio</i> pps <i>max-pps</i> kbps <i>max-kbps</i> } [unknown]	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 { <i>ratio</i> pps <i>max-pps</i> kbps <i>max-kbps</i> }	By default, unknown unicast traffic is allowed to pass through an interface.

Configuring storm control on an Ethernet interface

Storm control compares broadcast, multicast, and unknown 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 function.

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 <i>seconds</i>	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 <i>interface-type</i> <i>interface-number</i>	N/A
4. (Optional.) Enable storm control, and set the lower and upper thresholds for broadcast, multicast, or unknown unicast traffic.	storm-constrain { broadcast multicast unicast } { pps kbps ratio } <i>max-pps-values</i> <i>min-pps-values</i>	By default, storm control is disabled.
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 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.

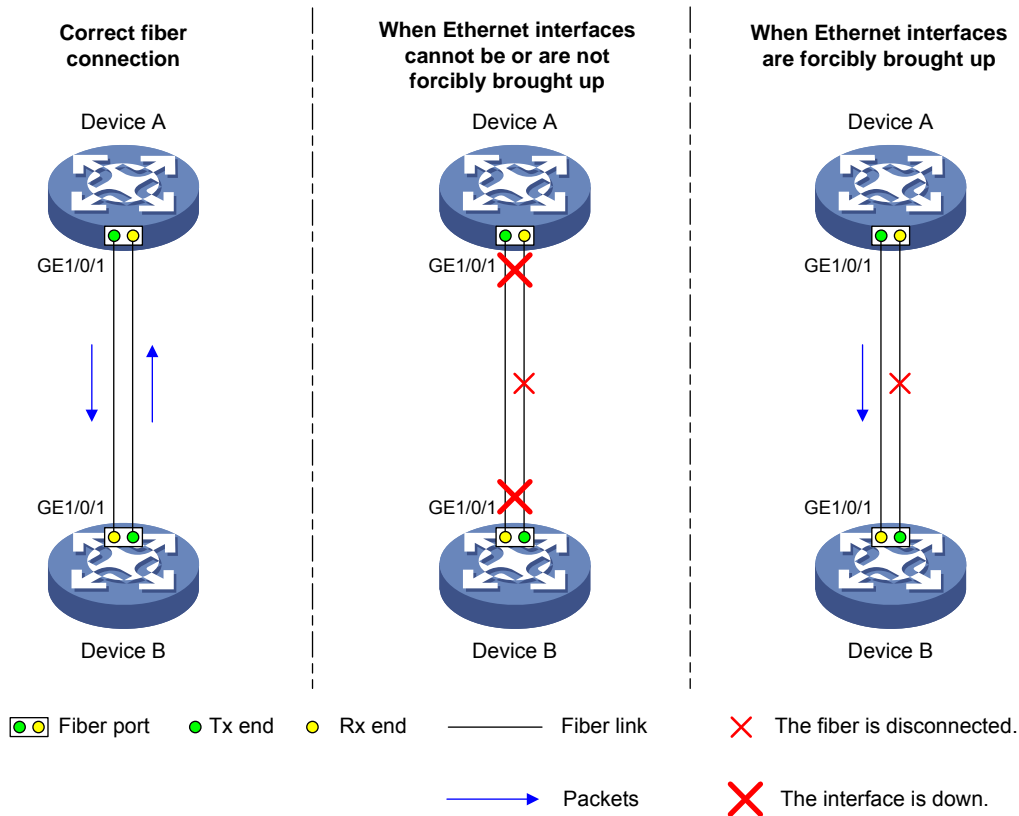
⚠ IMPORTANT:

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 the **shutdown** command.
- 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 <i>interface-type</i> <i>interface-number</i>	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.
- 10-GE copper ports support only the AutoMDIX mode of these MDIX modes.

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 <i>interface-type</i> <i>interface-number</i>	N/A
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 <i>interface-type interface-number</i>
3. Test the cable connected to the Ethernet interface.	virtual-cable-test

Enabling bridging on an Ethernet interface

ⓘ IMPORTANT:

This feature is available in Release 3113P05 and later versions.

By default, the device drops packets whose outgoing interface and incoming interface are the same.

To enable the device to forward such packets rather than drop them, enable the bridging feature in Ethernet interface view.

To enable bridging on an Ethernet interface:

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

Configuring speed downgrade autonegotiation

ⓘ IMPORTANT:

This feature is available in Release 3113P05 and later versions.

This feature is available only on GE interfaces.

Two GE interfaces configured with speed autonegotiation are connected through a network cable. When one end of the link supports only 100 Mbps because of network cable aging, the two interfaces still autonegotiate the speed as 1000 Mbps. As a result, the link cannot operate properly.

The speed downgrade autonegotiation feature downgrades the autonegotiated speed to 100 Mbps. Then, the link can operate properly.

To configure speed downgrade autonegotiation on an Ethernet interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type interface-number</i>	N/A
3. Enable speed downgrade autonegotiation on the Ethernet interface.	speed auto downgrade	By default, speed downgrade autonegotiation is enabled on an Ethernet interface.

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 [<i>interface-type</i> [<i>interface-number</i>]]
Display traffic rate statistics of interfaces in up state over the last sampling interval.	display counters rate { inbound outbound } interface [<i>interface-type</i> [<i>interface-number</i>]]
Display the operational and status information of the specified interface or all interfaces.	display interface [<i>interface-type</i> [<i>interface-number</i>]]
Display summary information about the specified interface or all interfaces.	display interface [<i>interface-type</i> [<i>interface-number</i>]] brief [description]
Display information about dropped packets on the specified interface or all interfaces.	display packet-drop { interface [<i>interface-type</i> [<i>interface-number</i>]] summary }
Display information about storm control on the specified interface or all interfaces.	display storm-constrain [broadcast multicast unicast] [interface <i>interface-type</i> <i>interface-number</i>]
Display the Ethernet statistics.	display ethernet statistics slot <i>slot-number</i>
Clear the interface statistics.	reset counters interface [<i>interface-type</i> [<i>interface-number</i>]]
Clear the statistics of dropped packets on the specified interfaces.	reset packet-drop interface [<i>interface-type</i> [<i>interface-number</i>]]
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.

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 <i>interface-number</i>	N/A
3. Set the interface description.	description <i>text</i>	The default setting is <i>interface name Interface</i> (for example, LoopBack1 Interface).
4. Configure the expected bandwidth of the loopback interface.	bandwidth <i>bandwidth-value</i>	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 <i>text</i>	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 [<i>interface-number</i>] [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 [<i>interface-number</i>]
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 only limited by the system resources. To guarantee bulk interface configuration performance, configure fewer than 1000 interface range names.
- If a command fails to be executed on the first interface in the interface range, the command is not executed on the other member interfaces. If the command fails to be executed on a non-first member interface, the system executes the command in system view:
 - If the execution succeeds, the system stays in system view, and leaves the bulk configuration process. The command is not executed on the subsequent member interfaces.
 - If the execution fails, the system enters interface range view, and continues to execute the command on the subsequent member interfaces.

Configuration procedure

To bulk configure interfaces:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface range view.	<ul style="list-style-type: none">• interface range { <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] } &<1-5>• interface range name <i>name</i> [interface { <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] } &<1-5>]	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.

Step	Command	Remarks
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.
- **Multipoint unicast entries**—A multipoint 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 multipoint unicast entry has higher priority than a dynamically learned one.

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

Configuring the 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 multipoint unicast MAC address entries. For information about configuring static multicast MAC address entries, see *IP Multicast Configuration Guide*.

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

Tasks at a glance
(Optional.) Configuring MAC address entries <ul style="list-style-type: none"> • 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 multipoint 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.) Enabling MAC address synchronization
(Optional.) Enable MAC address move notifications
(Optional.) Enabling ARP fast update for MAC address moves
(Optional.) Disabling static source check
(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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface interface-type interface-number Enter Layer 2 aggregate interface view: 	N/A

Step	Command	Remarks
	interface bridge-aggregation <i>interface-number</i>	
3. Add or modify a static or dynamic MAC address entry.	mac-address { dynamic static } <i>mac-address vlan vlan-id</i>	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 <i>mac-address vlan vlan-id</i>	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

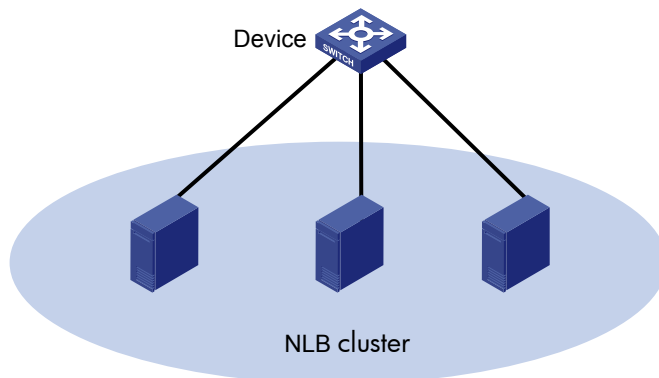
You can configure a multiport unicast MAC address entry to associate a unicast destination MAC address with multiple ports. The frame with a destination MAC address matching the entry is sent out of multiple ports.

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 <i>mac-address interface</i> <i>interface-list vlan vlan-id</i>	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.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i>Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i>	N/A
3. Add the interface to a multiport unicast MAC address entry.	mac-address multiport <i>mac-address vlan vlan-id</i>	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.

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.

When MAC address learning is disabled globally, the existing dynamic MAC address entries remain valid until they age out.

Disabling MAC address learning on an interface

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

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

To disable MAC address learning on an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i>Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i>	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.

When MAC address learning is disabled on a VLAN, the existing dynamic MAC address entries on the VLAN remain valid until they age out.

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 <i>vlan-id</i>	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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the MAC learning limit on the interface.	mac-address max-mac-count <i>count</i>	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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view. interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view. interface bridge-aggregation <i>interface-number</i> 	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.

Enabling MAC address synchronization

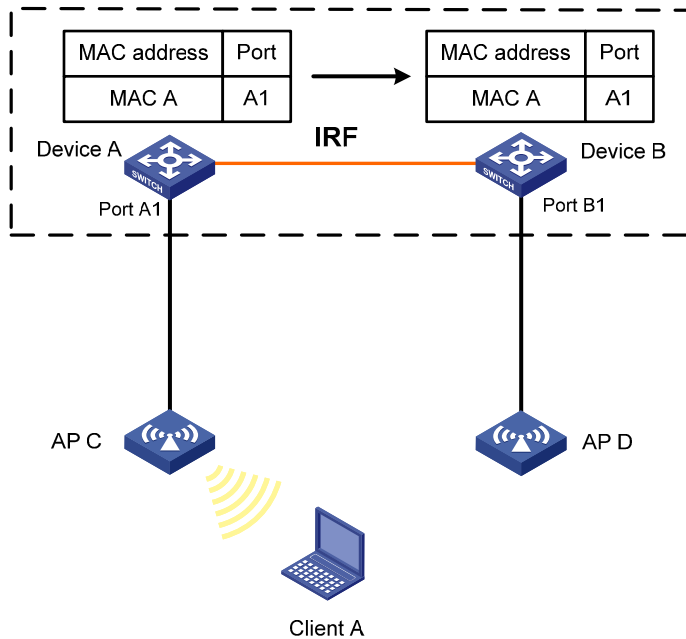
To avoid unnecessary floods and improve forwarding speed, make sure all member devices have the same MAC address table. After you enable MAC address synchronization, each member device advertises learned MAC address entries to other member devices.

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.

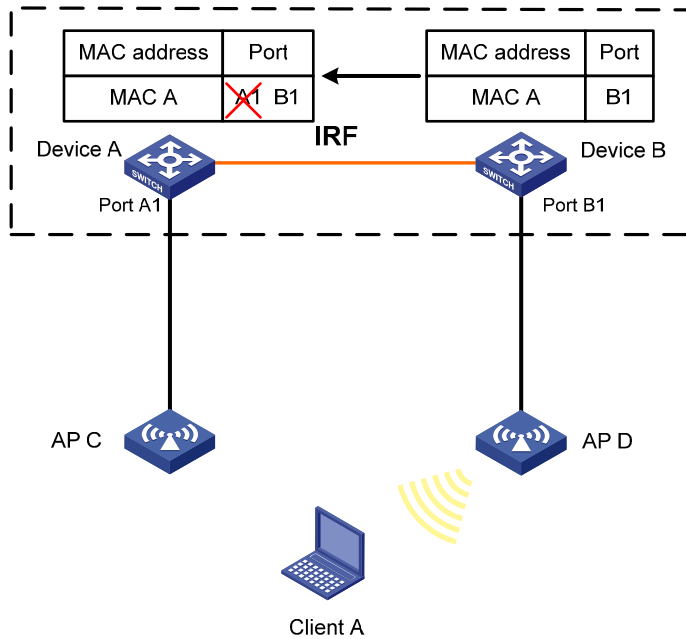
When Client A associates with AP C, Device A learns a MAC address entry for Client A and advertises it to Device B.

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:

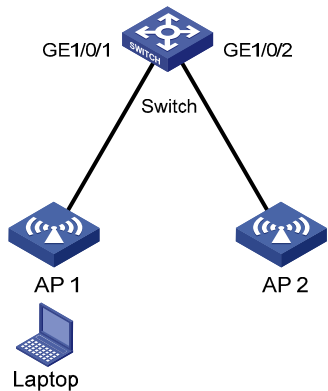
Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable MAC address move notifications and optionally specify a detection interval.	mac-address notification mac-move [interval <i>interval-value</i>]	By default, MAC address move notifications are disabled. If you do not specify a detection interval, the default setting of 1 minute is used. After you execute this command: <ul style="list-style-type: none"> If the device is configured with the snmp-agent trap enable mac-address command, the system sends SNMP notifications to the SNMP module. Otherwise, the system sends log messages to the information center module.
3. Set a threshold for MAC address moves sourced from an interface within a detection interval.	mac-address notification mac-move suppression threshold <i>threshold-value</i>	The default setting is 3.
4. Set a MAC address move suppression interval.	mac-address notification mac-move suppression interval <i>interval-value</i>	The default setting is 30 seconds.
5. Enter interface view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface: interface bridge-aggregation <i>interface-number</i> 	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.

Disabling static source check

By default, the static source check feature is enabled on an interface. The check identifies whether a received frame meets the following conditions:

- The source MAC address of the frame matches a static MAC address entry.
- The incoming interface of the frame is different from the outgoing interface in the entry.

If the frame meets both conditions, the switch drops the frame.

When this feature is disabled, the switch does not perform the check for a received frame. It can forward the frame whether or not the frame meets the conditions.

To disable the static source check feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> • Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	N/A
3. Disable the static source check feature.	undo mac-address static source-check enable	By default, the static source check feature is enabled.

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 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 [<i>mac-address</i> [vlan <i>vlan-id</i>]] [[dynamic static] [interface <i>interface-type</i> <i>interface-number</i>] blackhole multiport] [vlan <i>vlan-id</i>] [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 <i>interface-type</i> <i>interface-number</i>]
Display MAC address statistics.	display mac-address statistics
Display the MAC address move records.	display mac-address mac-move [slot <i>slot-number</i>]

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 table 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 <i>interface-type</i> <i>interface-number</i>	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 <i>interval-time</i>	The default setting is 1 second.

Configuring the MAC Information queue length

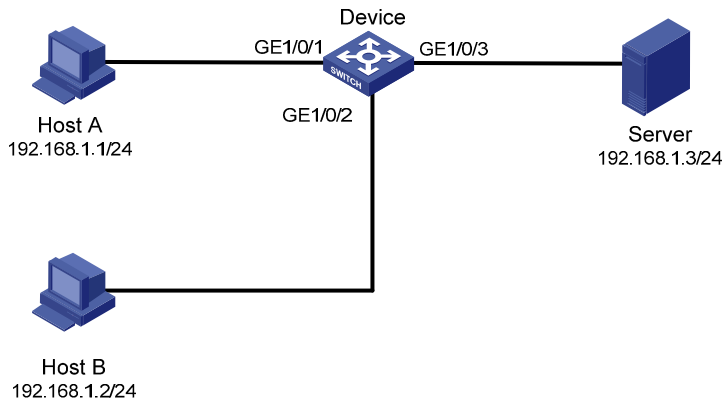
Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the MAC Information queue length.	mac-address information queue-length <i>value</i>	The default setting is 50.

MAC Information configuration example

Network requirements

Enable MAC Information on interface GigabitEthernet 1/0/1 on Device in [Figure 6](#) to send MAC address changes in syslog messages to the log host, Host B, through interface GigabitEthernet 1/0/2.

Figure 6 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:

- o Learns a new MAC address.
- o 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 7](#), 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 7 Ethernet link aggregation diagram



Basic concepts

Aggregation group, member port, and aggregate interface

An aggregation group is a group of Ethernet interfaces bundled together. These Ethernet interfaces are called member ports of the aggregation group. Each aggregation group has a corresponding logical interface (called an aggregate interface).

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.

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.

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 1](#) 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 might affect the aggregation state of link aggregation member ports and running services. The system displays a warning message every time you try to change an attribute configuration setting on a member port.

Table 1 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	<ul style="list-style-type: none">• 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**—Static Aggregation is stable. An aggregation group in static mode is called a static aggregation group. The aggregation state of the member ports in a static aggregation group are not affected by the peer ports.
- **Dynamic**—An aggregation group in dynamic mode is called a dynamic aggregation group. The local system and the peer system automatically maintain the aggregation states of the member ports. Dynamic link aggregation reduces the administrators' workload.

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:

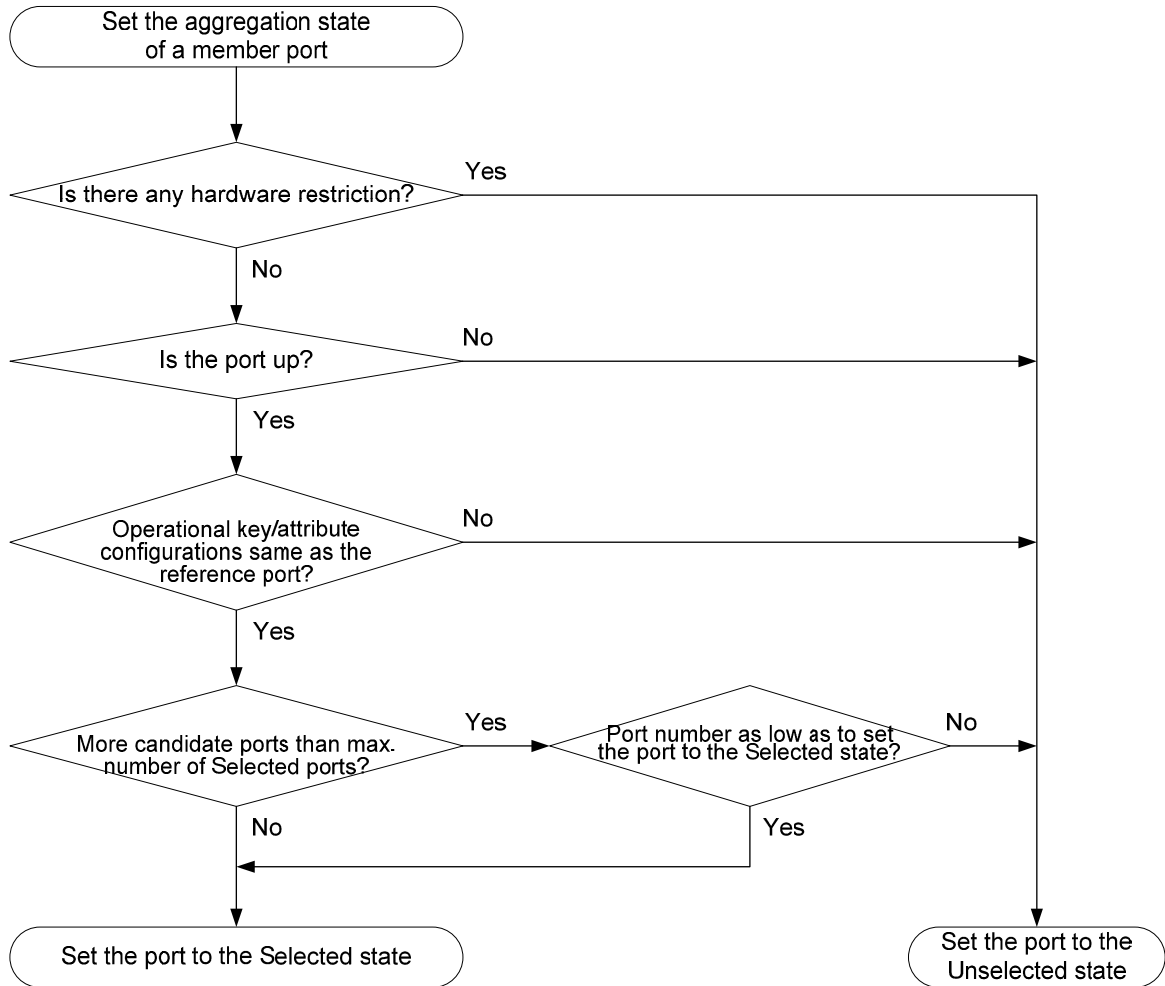
1. Highest port priority
2. Full duplex/high speed
3. Full duplex/low speed
4. Half duplex/high speed
5. Half duplex/low speed

The candidate port at the top is chosen as the reference port. If two ports have the same port priority, duplex mode, and speed, the original Selected port is chosen. If more than one such original Selected port exists, the one with the lower 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 8 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.

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 2](#).

Table 2 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 <i>IRF Configuration Guide</i> .

LACP priorities

LACP priorities include system LACP priority and port priority, as described in [Table 3](#). The smaller the priority value, the higher the priority.

Table 3 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 port state accordingly.
Port priority	Determines the likelihood of a member port to be selected on a system. The higher port priority, the higher the likelihood of selection.

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. You can configure the LACP timeout interval as the short timeout interval (3 seconds) or the long timeout interval (90 seconds). If you configure the short timeout interval, the peer sends LACPDUs fast (one LACPDU per second). If you configure the long timeout interval, the peer sends LACPDUs slowly (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:

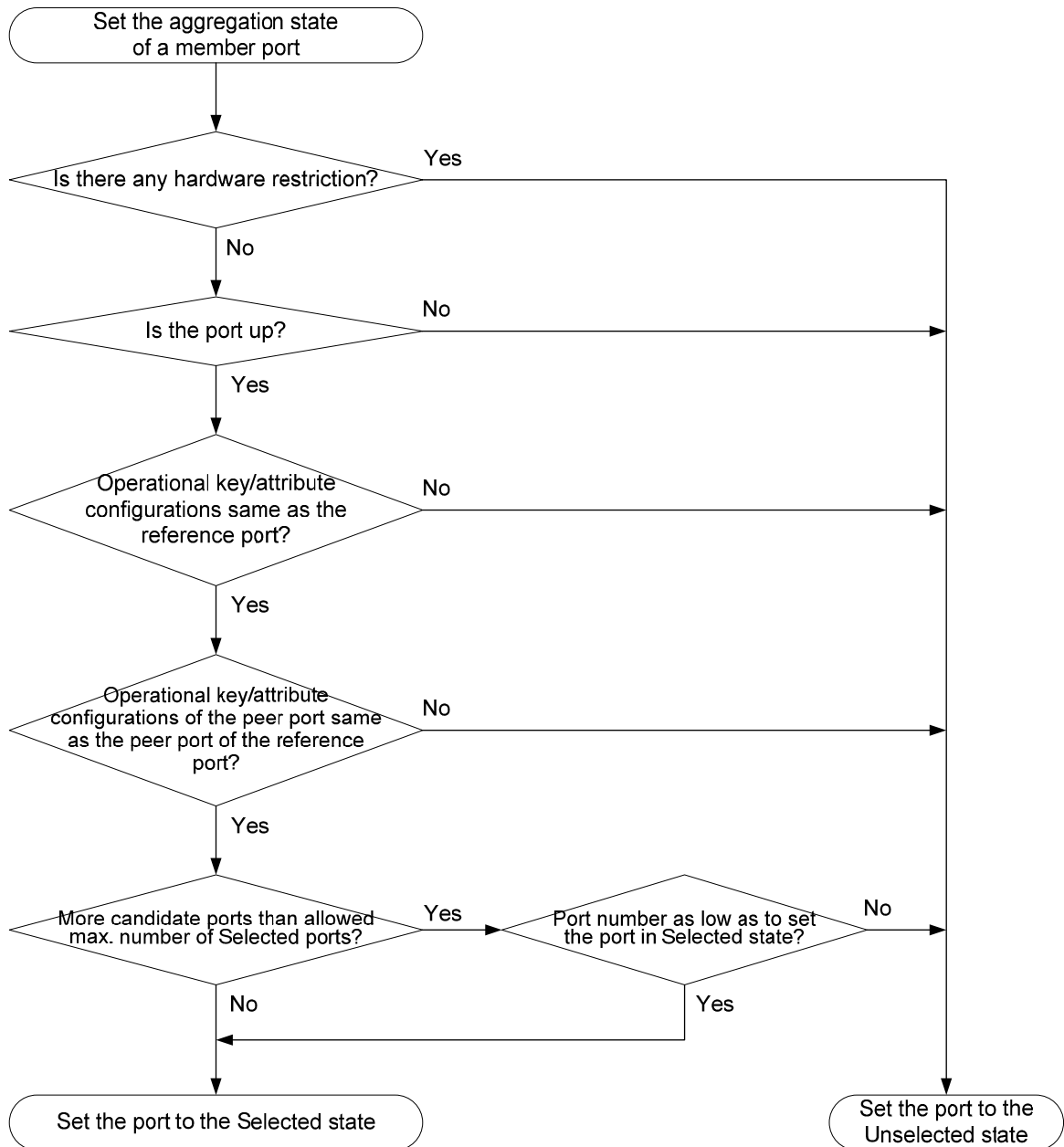
1. The systems compare their system IDs. (A system ID contains the system LACP priority and the system MAC address.) The lower the LACP priority, the smaller the system ID. If LACP priority values are the same, the two systems compare their MAC addresses. The lower the MAC address, the smaller the system 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 port with the lower priority value is chosen. If two ports have the same aggregation priority, the system compares their port numbers. The port with the smaller port number and the same attribute configurations as the aggregate interface becomes the reference port.

Setting the aggregation state of each member port

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

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



Meanwhile, 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 sets full-duplex ports as the Selected ports. The group will set only one half-duplex port as a Selected port when either of the following conditions exist:
 - None of the full-duplex ports can be selected.
 - 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.](#)"

Load sharing modes for link aggregation groups

In a link aggregation group, traffic may 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 traffic classification criteria:
 - 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: <ul style="list-style-type: none"> • Configuring a static aggregation group • Configuring a dynamic aggregation group
(Optional.) Configuring an aggregate interface: <ul style="list-style-type: none"> • Configuring the description of an aggregate interface • Specifying ignored VLANs for a Layer 2 aggregate interface • Setting the minimum and maximum numbers of Selected ports for an aggregation group • Setting the expected bandwidth of an aggregate interface • Enabling BFD for an aggregation group • Shutting down an aggregate interface • Restoring the default settings for an aggregate interface
(Optional.) Configuring load balancing for link aggregation group: <ul style="list-style-type: none"> • Setting load sharing modes for link aggregation groups • Enabling local-first load sharing for link aggregation
Enabling link-aggregation traffic redirection

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 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*).
- 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.

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
2. Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>	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 <i>interface-type</i> <i>interface-number</i> b. Assign the interface to the specified Layer 2 aggregation group: port link-aggregation group <i>number</i>	Repeat these two sub-steps to assign more Layer 2 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 <i>system-priority</i>	By default, the system LACP priority is 32768. Changing the system LACP priority might affect the aggregation state of the ports in a dynamic aggregation group.
3. Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>	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 <i>interface-type</i> <i>interface-number</i> b. Assign the interface to the specified Layer 2 aggregation group: port link-aggregation group <i>number</i>	Repeat these two sub-steps to assign more Layer 2 Ethernet interfaces to the aggregation group.
7. Configure the port priority for the interface.	link-aggregation port-priority <i>port-priority</i>	The default setting is 32768.
8. Configure the short LACP timeout interval (3 seconds) on the interface.	lacp period short	By default, the long LACP timeout interval (90 seconds) is adopted by the interface. The peer sends LACPDU slowly.

Configuring an aggregate interface

Most of the configurations that can be performed on Layer 2 Ethernet interfaces can also be performed on Layer 2 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 Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>	N/A
3. Configure the description of the aggregate interface.	description <i>text</i>	By default, the description of an interface is <i>interface-name</i> 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 <i>interface-number</i>	N/A
3. Specify ignored VLANs.	link-aggregation ignore vlan <i>vlan-id-list</i>	By default, a Layer 2 aggregate interface does not ignore any VLANs.

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

ⓘ IMPORTANT:

The minimum and maximum number 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 the 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 the configured maximum number or hardware capability, whichever value is smaller.

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

- Assign two ports to an aggregation group.
- Configure 1 as the maximum number of Selected ports allowed in the aggregation group.

Then, only one Selected port is allowed in the aggregation group at any point in time, and the Unselected port serves 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 Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>	N/A
3. Set the minimum number of Selected ports for the aggregation group.	link-aggregation selected-port minimum <i>number</i>	By default, the minimum number of Selected ports for the aggregation group is not specified.
4. Set the maximum number of Selected ports for the aggregation group.	link-aggregation selected-port maximum <i>number</i>	By default, the maximum number of Selected ports for an aggregation group is 8.

Setting the expected bandwidth of an aggregate interface

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

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. All the BFD sessions use UDP port 6784 and destination MAC address 01-00-5E-90-00-01. 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 the 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 the 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 the 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.

To enable BFD for an aggregation group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>	N/A
3. Enable BFD for the aggregation group.	link-aggregation bfd ipv4 source <i>ip-address</i> destination <i>ip-address</i>	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 Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>
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 Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>
3. Restore the default settings for the aggregate interface.	default

Configuring load sharing for link aggregation groups

This section explains how to configure load sharing modes for link aggregation groups and how to enable local-first load sharing for link aggregation.

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

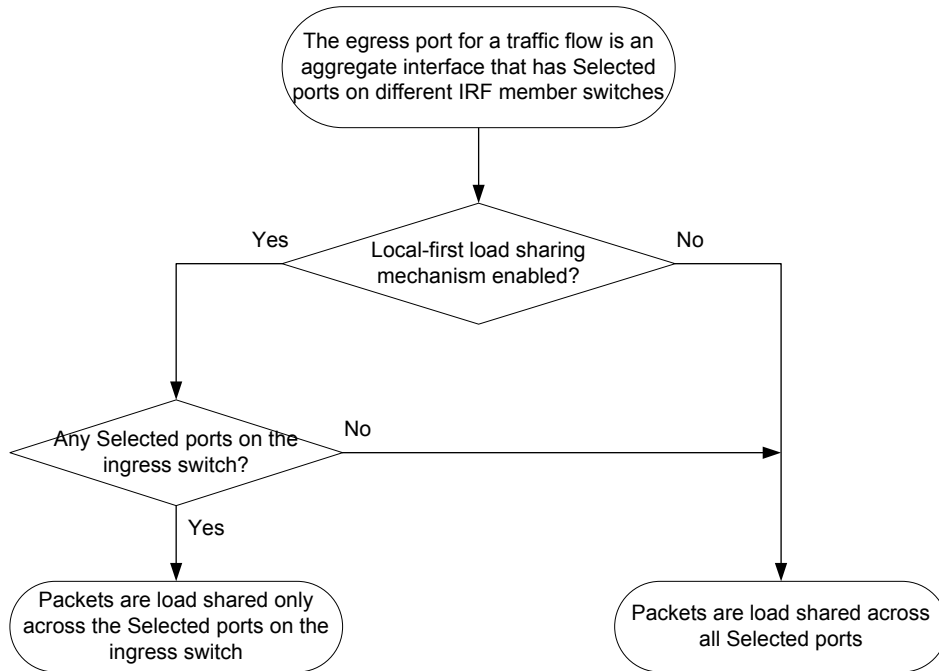
Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 aggregate interface view.	interface bridge-aggregation <i>interface-number</i>	N/A
3. Configure the load sharing mode for the aggregation group.	link-aggregation load-sharing mode { destination-ip destination-mac source-ip source-mac } *	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 10](#). For more information about IRF, see *IRF Configuration Guide*.

Figure 10 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.

Enabling link-aggregation traffic redirection

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.

Configuration restrictions and guidelines

When you enable link-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.

Configuration procedure

To enable link-aggregation traffic redirection:

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

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] [brief [down]] display interface [bridge-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 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 [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 [interface-number]]

Ethernet link aggregation configuration examples

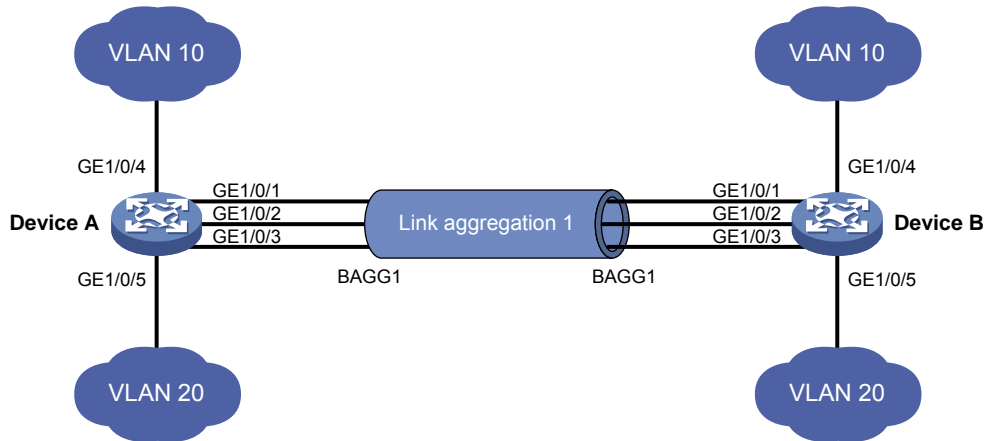
Layer 2 static aggregation configuration example

Network requirements

As shown in [Figure 11](#):

- 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 11 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.

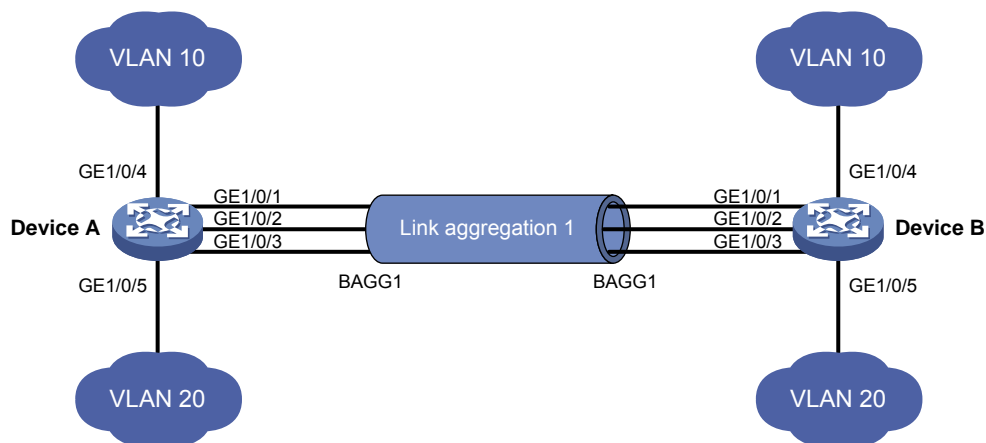
Layer 2 dynamic aggregation configuration example

Network requirements

As shown in [Figure 12](#):

- 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 12 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.

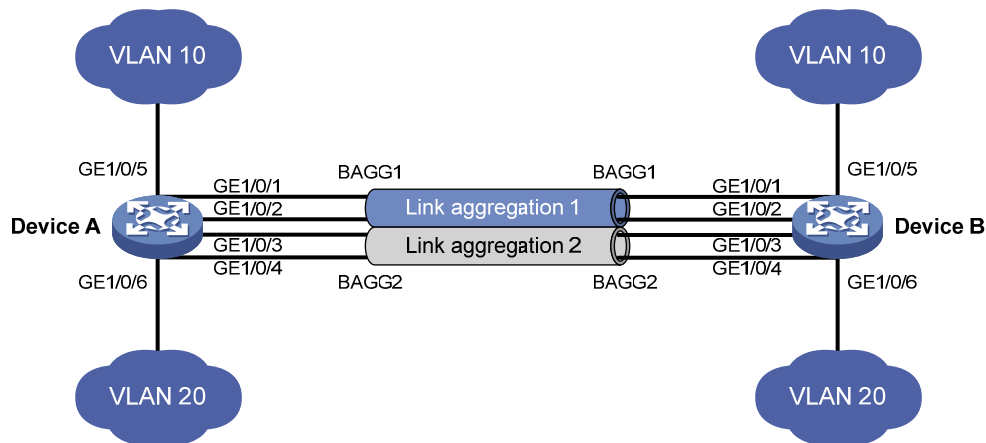
Layer 2 aggregation load sharing configuration example

Network requirements

As shown in [Figure 13](#):

- Configure Layer 2 static aggregation groups 1 and 2 on 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.
- 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 13 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.

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 <i>group-number</i>	By default, no isolation group exists.
3. Enter interface view.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i>Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i>	<ul style="list-style-type: none">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 <i>group-number</i>	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 [<i>group-number</i>]

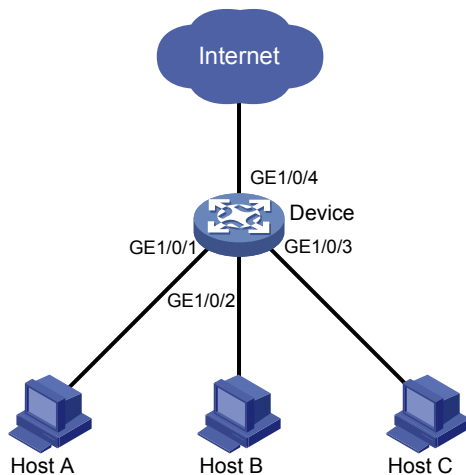
Port isolation configuration example

Network requirements

As shown in Figure 14, 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 14 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 15](#), Device B and Device C are directly connected to a LAN.

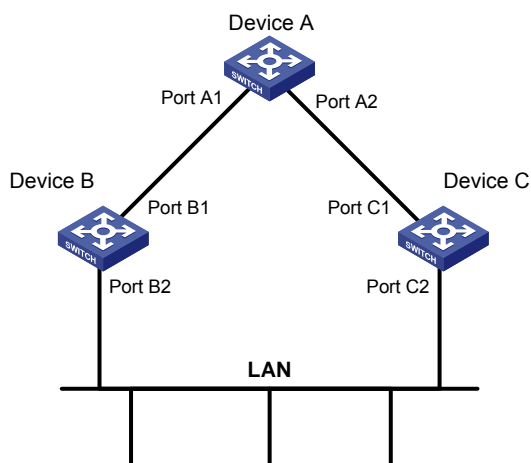
If Device A forwards BPDUs to Device B through port A1:

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

Figure 15 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 a simplified process for example only.

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 4 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. <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• If the calculated configuration BPDU is superior, the device performs the following tasks:<ul style="list-style-type: none">○ 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 4 Selecting the optimum configuration BPDU

Step	Actions
1	<p>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.</p> <ul style="list-style-type: none"> • 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:

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

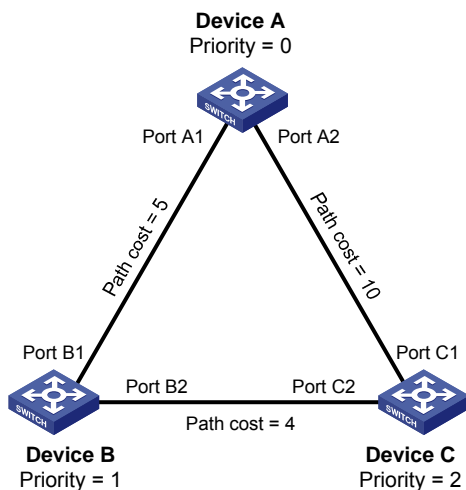
The configuration BPDU that contains a smaller designated bridge ID, designated port ID, or receiving port ID is selected.

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

Example of STP calculation

Figure 16 provides an example showing how the STP algorithm works.

Figure 16 The STP algorithm



As shown in Figure 16, 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 5, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

Table 5 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 6](#), each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

Table 6 Comparison process and result on each device

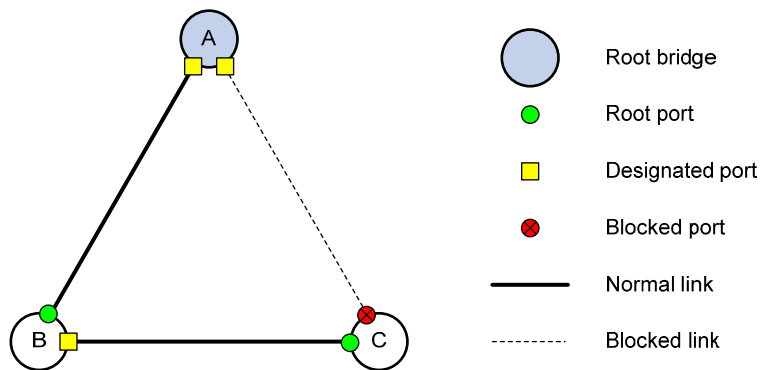
Device	Comparison process	Configuration BPDU on ports after comparison
Device A	<p>Port A1 performs the following tasks:</p> <ol style="list-style-type: none"> 1. Receives the configuration BPDU of Port B1 {1, 0, 1, Port B1}. 2. Determines that its existing configuration BPDU {0, 0, 0, Port A1} is superior to the received configuration BPDU. 3. Discards the received one. <p>Port A2 performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>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.</p>	<ul style="list-style-type: none"> • Port A1: {0, 0, 0, Port A1} • Port A2: {0, 0, 0, Port A2}
Device B	<p>Port B1 performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>Port B2 performs the following tasks:</p> <ol style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> • Port B1: {0, 0, 0, Port A1} • Port B2: {1, 0, 1, Port B2}

Device	Comparison process	Configuration BPDU on ports after comparison
	<p>Device B performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>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.</p>	<ul style="list-style-type: none"> • Root port (Port B1): {0, 0, 0, Port A1} • Designated port (Port B2): {0, 5, 1, Port B2}
Device C	<p>Port C1 performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>Port C2 performs the following tasks:</p> <ol style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> • Port C1: {0, 0, 0, Port A2} • Port C2: {1, 0, 1, Port B2}
	<p>Device C performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>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.</p>	<ul style="list-style-type: none"> • Root port (Port C1): {0, 0, 0, Port A2} • Designated port (Port C2): {0, 10, 2, Port C2}
	<p>Port C2 performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>Port C1 performs the following tasks:</p> <ol style="list-style-type: none"> 1. Receives a periodic configuration BPDU {0, 0, 0, Port A2} from Port A2. 2. Determines that it is the same as the existing 	<ul style="list-style-type: none"> • Port C1: {0, 0, 0, Port A2} • Port C2: {0, 5, 1, Port B2}

Device	Comparison process	Configuration BPDU on ports after comparison
	<p>configuration BPDU.</p> <p>3. Discards the received BPDU.</p>	
	<p>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.</p> <p>Based on the configuration BPDU and path cost of the root port, Device C performs the following tasks:</p> <ol style="list-style-type: none"> 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. <p>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.</p>	<ul style="list-style-type: none"> • Blocked port (Port C1): {0, 0, 0, Port A2} • Root port (Port C2): {0, 5, 1, Port B2}

After the comparison processes described in Table 6, a spanning tree with Device A as the root bridge is established, as shown in Figure 17.

Figure 17 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 18 shows a switched network that comprises four MST regions, each MST region comprising four MSTP devices. Figure 19 shows the networking topology of MST region 3.

Figure 18 Basic concepts in MSTP

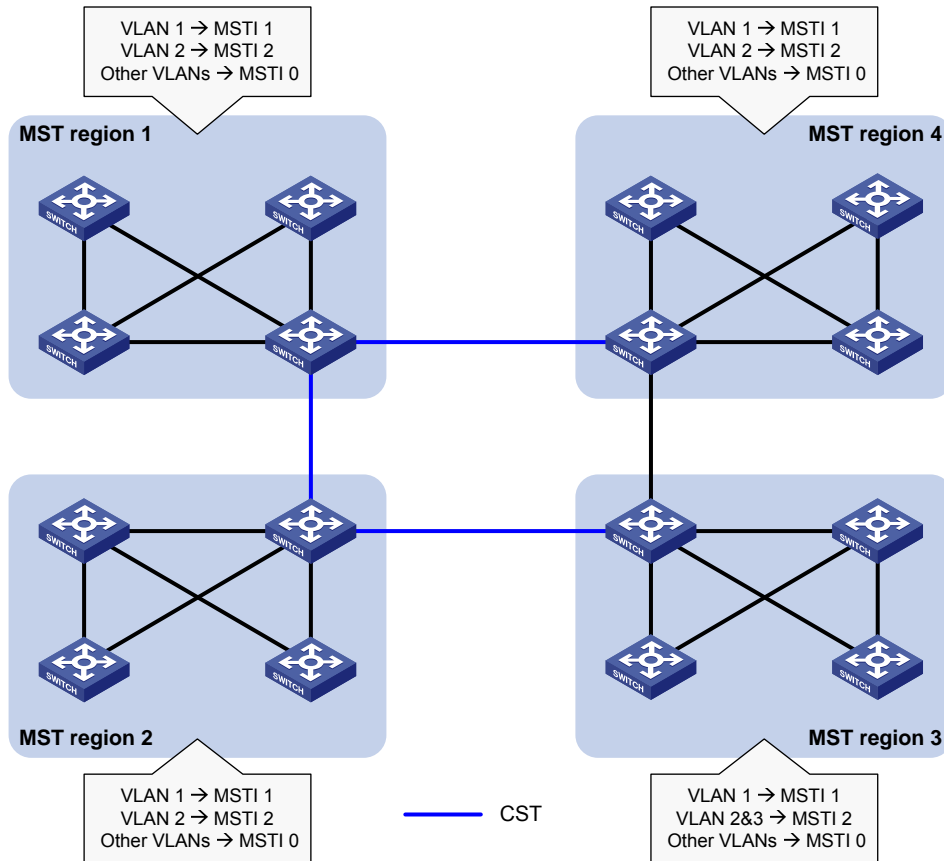
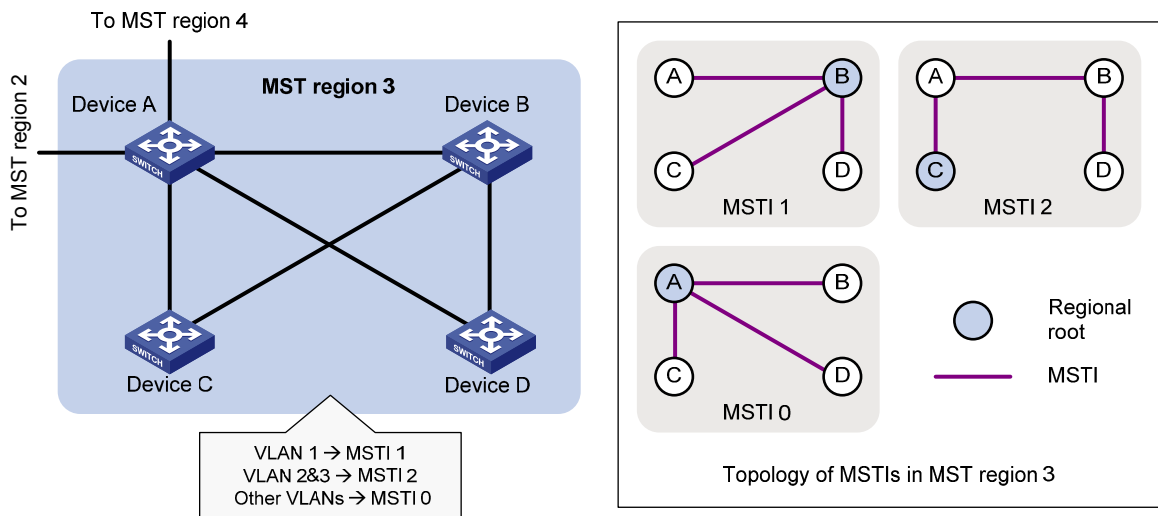


Figure 19 Network diagram and topology of MST region 3



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. In [Figure 18](#):

- 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 19](#), 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 19](#), 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 18](#) 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 18](#), 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 18](#), 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.

In MST region 3 in [Figure 19](#):

- 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

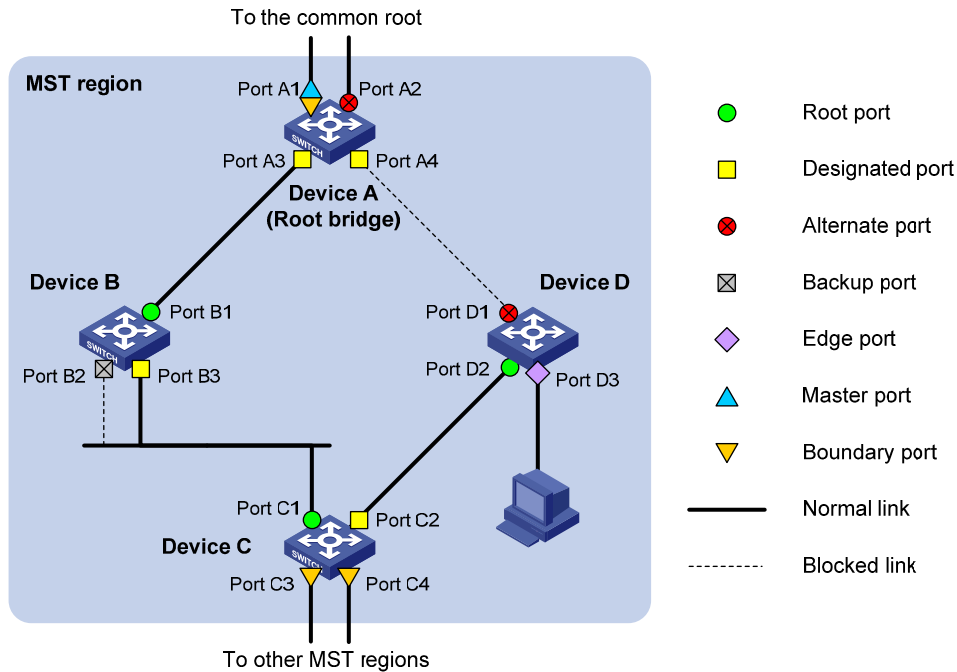
The common root bridge is the root bridge of the CIST.

In [Figure 18](#), 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 20](#), 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 20 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**—Serves 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**—Serves 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**—Serves 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 7](#) 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 7 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 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: <ul style="list-style-type: none"> • (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.) Setting spanning tree timers • (Optional.) Setting 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: <ul style="list-style-type: none"> • (Required.) Setting the spanning tree mode • (Optional.) Configuring the device priority • (Optional.) Setting 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
(Optional.) Enabling SNMP notifications for new-root election and topology change events

RSTP configuration task list

Tasks at a glance
Configuring the root bridge: <ul style="list-style-type: none"> • (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.) Setting spanning tree timers • (Optional.) Setting 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: <ul style="list-style-type: none"> • (Required.) Setting the spanning tree mode

Tasks at a glance
<ul style="list-style-type: none"> • (Optional.) Configuring the device priority • (Optional.) Setting 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 TC Snooping
(Optional.) Configuring protection functions
(Optional.) Enabling SNMP notifications for new-root election and topology change events

PVST configuration task list

Tasks at a glance
<p>Configuring the root bridge:</p> <ul style="list-style-type: none"> • (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.) Setting spanning tree timers • (Optional.) Setting 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
<p>Configuring the leaf nodes:</p> <ul style="list-style-type: none"> • (Required.) Setting the spanning tree mode • (Optional.) Configuring the device priority • (Optional.) Setting 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
(Optional.) Enabling SNMP notifications for new-root election and topology change events

MSTP configuration task list

Tasks at a glance
Configuring the root bridge: <ul style="list-style-type: none">• (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• (Optional.) Configuring the maximum hops of an MST region• (Optional.) Configuring the network diameter of a switched network• (Optional.) Setting spanning tree timers• (Optional.) Setting 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: <ul style="list-style-type: none">• (Required.) Setting the spanning tree mode• (Required.) Configuring an MST region• (Optional.) Configuring the device priority• (Optional.) Setting 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
(Optional.) Enabling SNMP notifications for new-root election and topology change events

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 number of spanning trees that a device can maintain is 128.

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.

Configuration restrictions and guidelines

When you make configurations in different spanning tree modes, follow these restrictions and guidelines:

- In STP or RSTP mode, do not specify an MSTI or VLAN. Otherwise, the spanning tree configuration does not take effect.
- In PVST mode, if you specify a VLAN, the spanning tree configuration takes effect on the specified VLAN. Otherwise, the spanning tree configuration does not take effect.
- In MSTP mode, if you specify an MSTI, the spanning tree configuration takes effect on the specified MSTI. If you do not specify an MSTI or VLAN, the spanning tree configuration takes effect on the CIST.

Configuration procedure

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 <i>name</i>	The default setting is the MAC address.
4. Configure the VLAN-to-instance mapping table.	<ul style="list-style-type: none"> • instance <i>instance-id</i> vlan <i>vlan-id-list</i> • vlan-mapping modulo <i>modulo</i> 	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 <i>level</i>	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 region configuration.	active region-configuration	N/A

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:

- 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.	<ul style="list-style-type: none"> 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
2. Configure the current device as a secondary root bridge.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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 <i>hops</i>	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.	<ul style="list-style-type: none">• In STP/RSTP/MSTP mode: stp bridge-diameter <i>diameter</i>• In PVST mode: stp vlan <i>vlan-id-list</i> bridge-diameter	The default setting is 7.

Step	Command	Remarks
	<i>diameter</i>	

Setting 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:

- $2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age}$
- $\text{Max age} \geq 2 \times (\text{hello time} + 1 \text{ second})$

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

Set 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 set the spanning tree timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the forward delay timer.	<ul style="list-style-type: none"> 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. Set the hello timer.	<ul style="list-style-type: none"> 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. Set the max age timer.	<ul style="list-style-type: none"> 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.

Setting the timeout factor

The timeout factor is a parameter used to decide the timeout period. The formula for calculating the timeout period is: $\text{timeout period} = \text{timeout factor} \times 3 \times \text{hello time}$.

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 set the timeout factor:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the BPDU transmission rate of the ports.	stp transmit-limit <i>limit</i>	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 <i>interface-type</i> <i>interface-number</i>	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 8 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		500000	1400

Link speed	Port type	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	Private standard
	containing four Selected ports			
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 ports		5000	14
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		166	1

Link speed	Port type	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	Private standard
100 Gbps	containing three Selected ports	1		
	Aggregate interface containing four Selected ports		125	1
	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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the path cost of the ports.	<ul style="list-style-type: none"> In STP/RSTP mode: stp cost <i>cost</i> In PVST mode: stp vlan <i>vlan-id-list</i> cost <i>cost</i> In MSTP mode: stp [instance <i>instance-list</i>] cost <i>cost</i> 	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 <i>interface-type interface-number</i>	N/A
3. Configure the port priority.	<ul style="list-style-type: none">• In STP/RSTP mode: stp port priority <i>priority</i>• In PVST mode: stp vlan <i>vlan-id-list</i> port priority <i>priority</i>• In MSTP mode: stp [instance <i>instance-list</i>] port priority <i>priority</i>	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 for the device to 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 <i>interface-type</i> <i>interface-number</i>	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.

A port in **auto** mode sends 802.1s MSTP packets by default. 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 <i>interface-type</i> <i>interface-number</i>	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.	<ul style="list-style-type: none"> In STP/RSTP mode: stp port-log instance 0 In PVST mode: stp port-log vlan <i>vlan-id-list</i> In MSTP mode: stp port-log { all instance <i>instance-list</i> } 	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	<ul style="list-style-type: none"> 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. <p>For more information about the startup configuration, see <i>Fundamentals Configuration Guide</i>.</p>
3. Enter Layer 2 Ethernet or aggregate interface view.	interface <i>interface-type</i> <i>interface-number</i>	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	<ul style="list-style-type: none">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 <i>Fundamentals Configuration Guide</i> .
3. Enable the spanning tree feature in VLANs.	stp vlan <i>vlan-id-list</i> enable	The spanning tree feature is enabled for all VLANs.
4. Enter Layer 2 Ethernet or aggregate interface view.	interface <i>interface-type</i> <i>interface-number</i>	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

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 <i>interface-type interface-number</i>
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 occur.

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 <i>interface-type</i> <i>interface-number</i>	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.

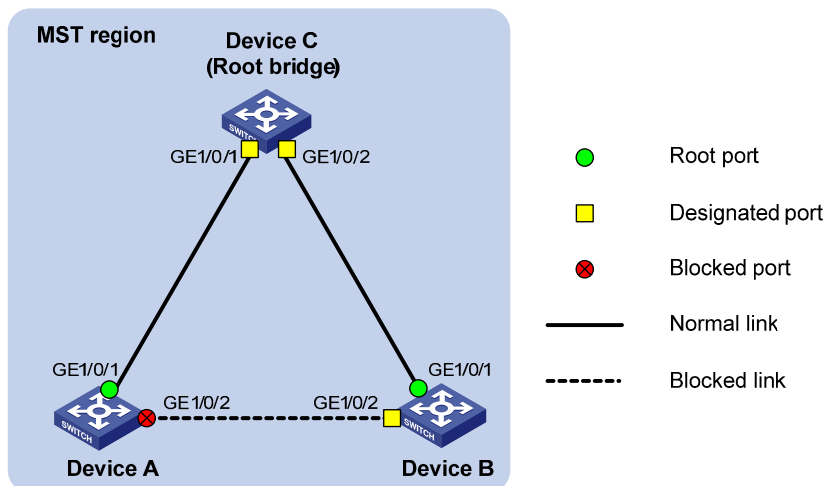
Digest Snooping configuration example

Network requirements

As shown in [Figure 21](#), 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 21 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 22 Rapid state transition of an MSTP designated port

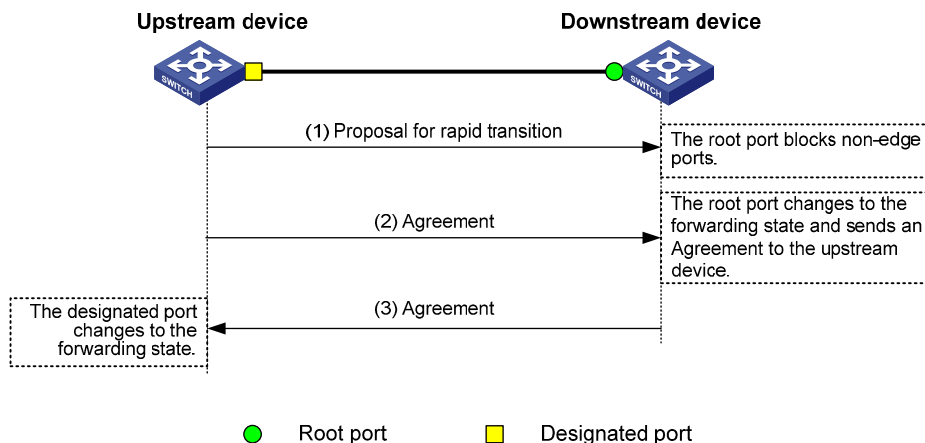
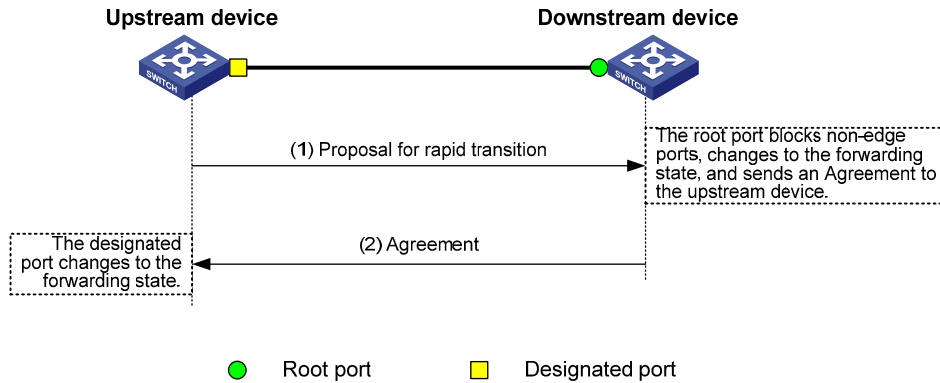


Figure 23 Rapid state transition of an RSTP designated port



If the upstream device is a third-party device, the rapid state transition implementation might be limited. For example:

- 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable No Agreement Check.	stp no-agreement-check	By default, No Agreement Check is disabled.

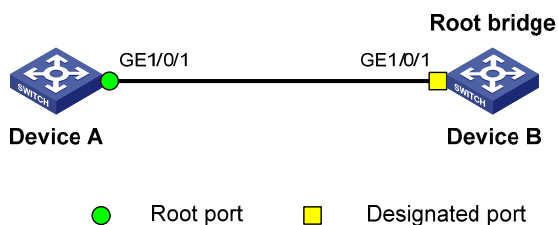
No Agreement Check configuration example

Network requirements

As shown in [Figure 24](#):

- 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 24 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
```

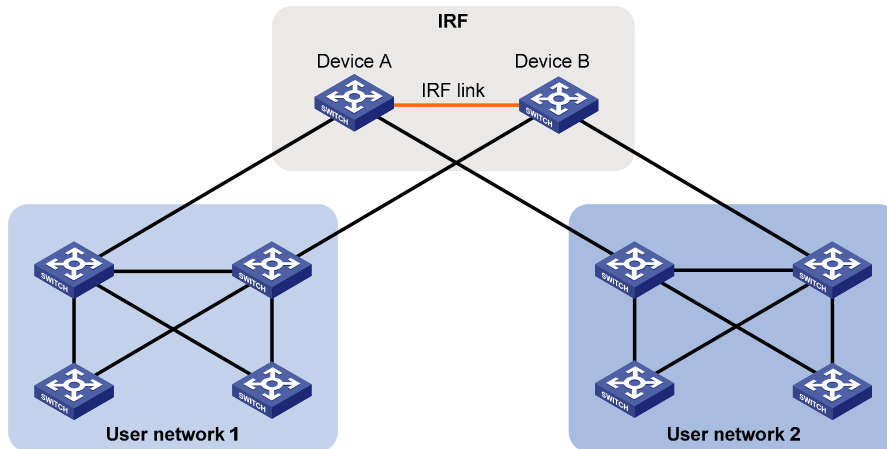
Configuring TC Snooping

As shown in [Figure 25](#):

- 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.
- User network 1 and user network 2 are connected to the IRF fabric through double links.
- 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 25 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	<ul style="list-style-type: none"> • 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. <p>For more information about the startup configuration, see <i>Fundamentals Configuration Guide</i>.</p>
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 <i>interface-type interface-number</i>	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 <i>interface-type interface-number</i>	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 <i>interface-type</i> <i>interface-number</i>	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 <i>interface-type</i> <i>interface-number</i>	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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable BPDU drop on the current interface.	bpdu-drop any	By default, BPDU drop is disabled.

Enabling SNMP notifications for new-root election and topology change events

This feature enables the device to generate logs and report new-root election events or spanning tree topology changes to SNMP. For the event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

When you use the **snmp-agent trap enable stp [new-root | tc]** command, follow these guidelines:

- The **new-root** keyword applies only to STP, MSTP, and RSTP modes.
- The **tc** keyword applies only to PVST mode.
- In STP, MSTP, or RSTP mode, the **snmp-agent trap enable stp** command enables SNMP notifications for new-root election events.
- In PVST mode, the **snmp-agent trap enable stp** command enables SNMP notifications for spanning tree topology changes.

To enable SNMP notifications for new-root election and topology change events:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable SNMP notifications for new-root election events.	In STP, MSTP, or RSTP mode, execute either of the following commands: <ul style="list-style-type: none"> snmp-agent trap enable stp new-root snmp-agent trap enable stp 	The default settings are as follows: <ul style="list-style-type: none"> SNMP notifications are disabled for new-root election events. In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes. In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.
3. Enable SNMP notifications for spanning tree topology changes.	In PVST mode, execute either of the following commands: <ul style="list-style-type: none"> snmp-agent trap enable stp tc snmp-agent trap enable stp 	
4. Enable the device to generate a log when it detects or receives a TCN BPDU in PVST mode.	stp log enable tc	By default, the device does not generate a log when it detects or receives a TCN BPDU in PVST mode.

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 <i>interface-type interface-number</i> [instance <i>instance-list</i>]]
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 <i>instance-list</i> vlan <i>vlan-id-list</i>] history [slot <i>slot-number</i>]
Display the statistics of TC/TCN BPDUs sent and received by all ports in the specified MSTI or all MSTIs.	display stp [instance <i>instance-list</i> vlan <i>vlan-id-list</i>] tc [slot <i>slot-number</i>]
Display the spanning tree status and statistics.	display stp [instance <i>instance-list</i> vlan <i>vlan-id-list</i>] [interface <i>interface-list</i> slot <i>slot-number</i>] [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 <i>interface-list</i>]

Spanning tree configuration example

MSTP configuration example

Network requirements

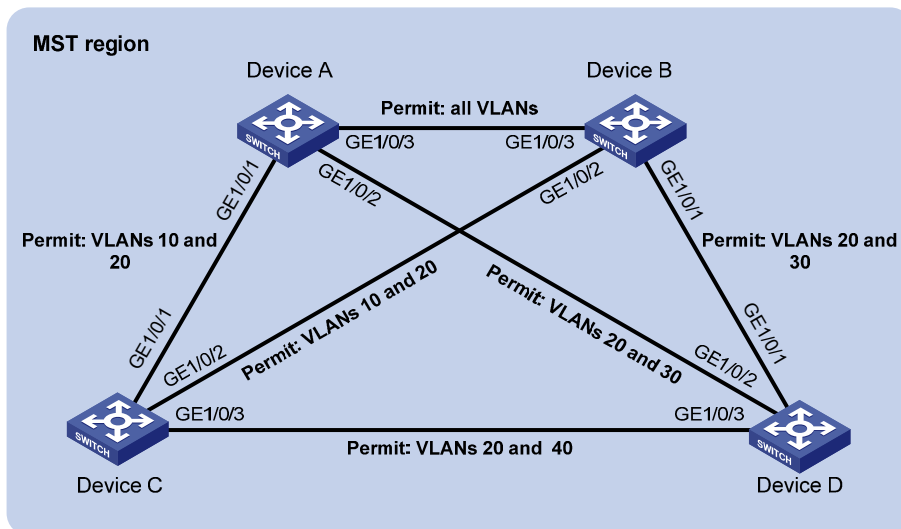
As shown in Figure 26, all devices on the network are in the same MST region. Device A and Device B work at the distribution layer. Device C and Device D work at the access layer.

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 26 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

```

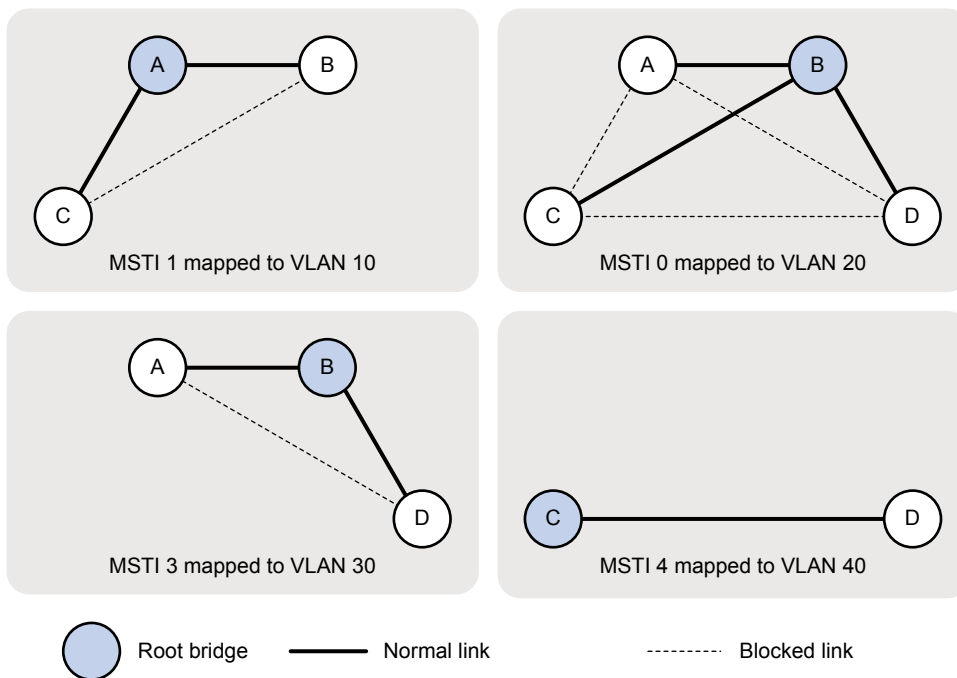
Display brief spanning tree information on Device D.

```
[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 27](#).

Figure 27 MSTIs mapped to different VLANs



PVST configuration example

Network requirements

As shown in [Figure 28](#):

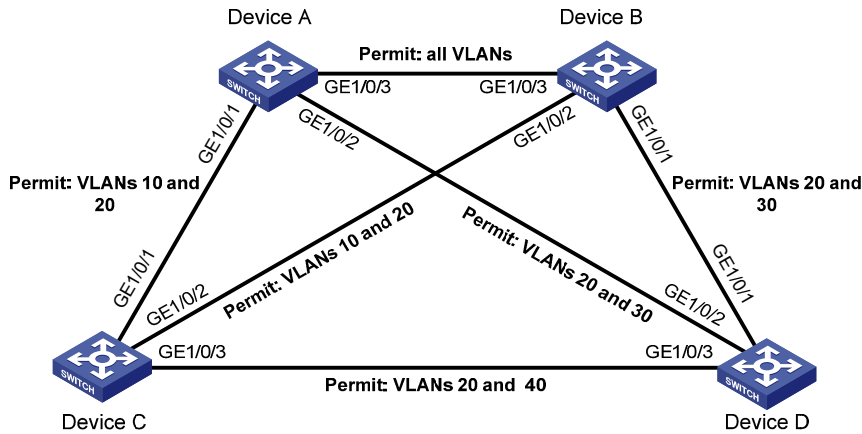
- Device A and Device B work at the distribution layer.
- Device C and Device D work at the access layer.

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 28 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.
```

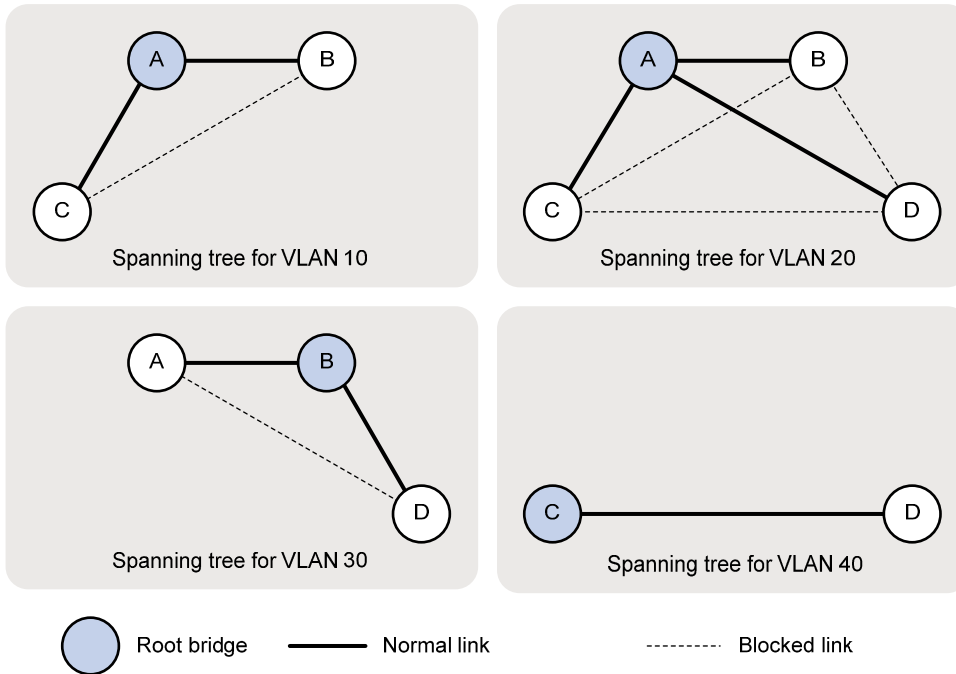
```
[DeviceD] display stp brief
```

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 29](#).

Figure 29 VLAN spanning tree topologies



Configuring L2PT

Overview

Layer 2 Protocol Tunneling (L2PT) can transparently send Layer 2 protocol packets from geographically dispersed customer networks across a service provider network.

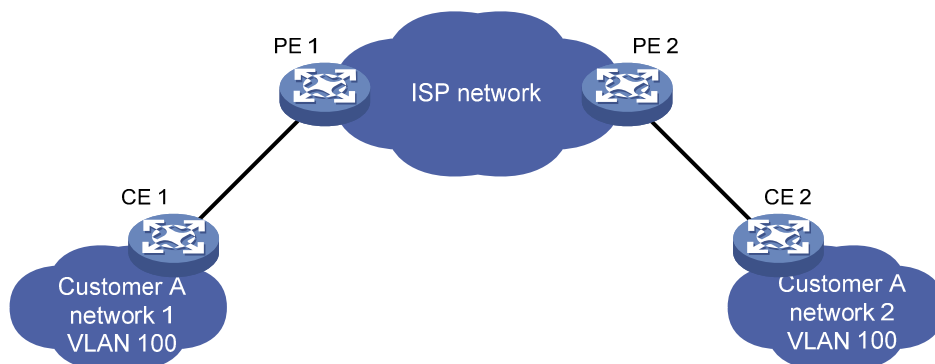
Background

Dedicated lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a customer network contains sites located at different sides of the service provider network.

As shown in [Figure 30](#), Customer A's network is divided into network 1 and network 2, which are connected by the service provider network. For Customer A's network to implement Layer 2 protocol calculations, the Layer 2 protocol packets must be transmitted across the service provider network.

Upon receiving a Layer 2 protocol packet, the PEs cannot determine whether the packet is from the customer network or the service provider network. They must deliver the packet to the CPU for processing. In this case, the Layer 2 protocol calculation in Customer A's network is mixed with the Layer 2 protocol calculation in the service provider network. Neither the customer network nor the service provider network can implement independent Layer 2 protocol calculations.

Figure 30 L2PT application scenarios



L2PT is introduced to resolve the problem. L2PT provides the following functions:

- Multicasts Layer 2 protocol packets from a customer network in a VLAN. Dispersed customer networks can complete an independent Layer 2 protocol calculation, which is transparent to the service provider network.
- Isolates Layer 2 protocol packets from different customer networks through different VLANs.

HPE devices support L2PT for the following protocols:

- CDP.
- DLDP.
- EOAM.
- GVRP.
- LACP.
- LLDP.
- MVRP.
- PAgP.

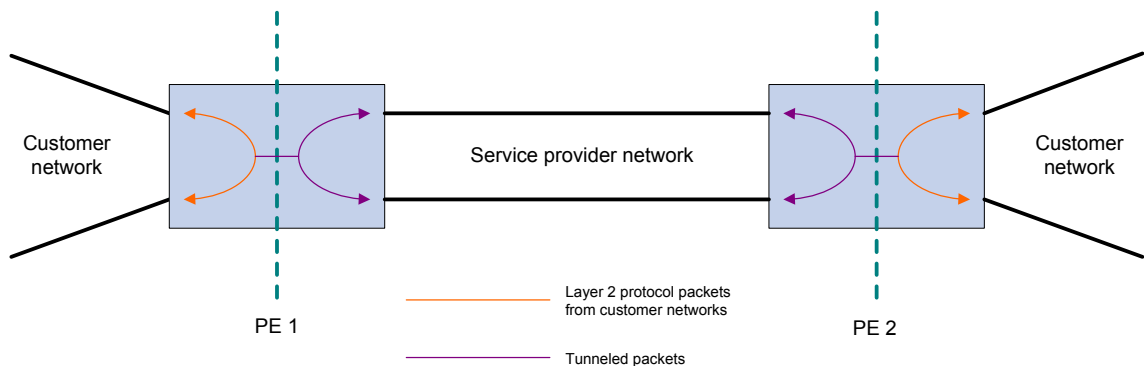
- PVST.
- STP (including STP, RSTP, and MSTP).
- VTP.

L2PT operating mechanism

As shown in [Figure 31](#), L2PT operates as follows:

- When a port of PE 1 receives a Layer 2 protocol packet from the customer network in a VLAN, it performs the following operations:
 - Multicasts the packet out of all customer-facing ports in the VLAN except the receiving port.
 - Changes the packet's destination multicast MAC address to a specified multicast address, and multicasts it out of all ISP-facing ports in the VLAN. The modified packet is called the tunneled packet.
- When a port of PE 1 in the VLAN receives the tunneled packet from the service provider network, it performs the following operations:
 - Multicasts the packet out of all ISP-facing ports in the VLAN except the receiving port.
 - Changes the destination multicast MAC address to the original MAC address, and multicasts the packet out of all customer-facing ports in the VLAN.

Figure 31 L2PT operating mechanism

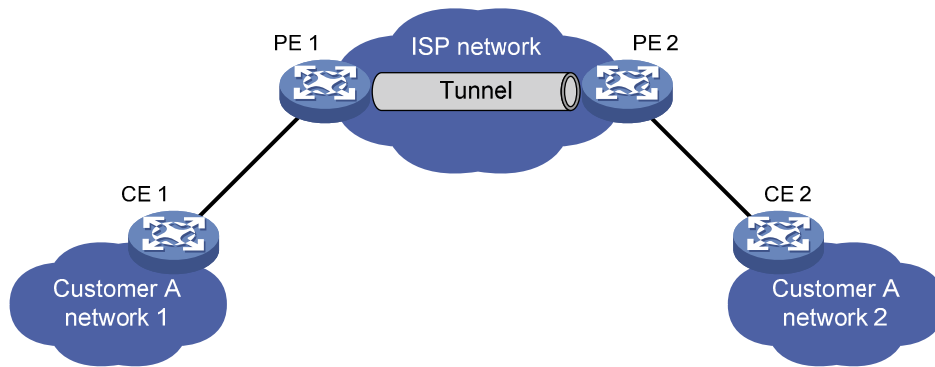


For example, as shown in [Figure 32](#), PE 1 receives an STP packet (BPDU) from network 1 to network 2. CEs are the edge devices on the customer network, and PEs are the edge devices on the service provider network. L2PT processes the packet as follows:

1. PE 1 performs the following operations:
 - a. Changes the packet's destination multicast MAC address 0180-c200-0000 to a specified multicast MAC address (010f-e200-0003 by default) for the BPDU.
 - b. Sends the tunneled packet out of all ISP-facing ports in the packet's VLAN.
2. Upon receiving the tunneled packet, PE 2 decapsulates the packet and sends the BPDU to CE 2.

Through L2PT, both the ISP network and Customer A's network can perform independent spanning tree calculations.

Figure 32 L2PT network diagram



L2PT configuration task list

Tasks at a glance
(Required.) Enabling L2PT
(Optional.) Setting the destination multicast MAC address for tunneled packets

Enabling L2PT

Restrictions and guidelines

- Before you enable L2PT for a Layer 2 protocol on a port, perform the following tasks:
 - Enable the protocol on the connected CE, and disable the protocol on the port.
 - Enable L2PT on PE ports connected to a customer network. If you enable L2PT on ports connected to the service provider network, L2PT determines that the ports are connected to a customer network.
 - Make sure the VLAN tags of Layer 2 protocol packets are not changed or deleted for the tunneled packets to be transmitted correctly across the service provider network.
- L2PT for LLDP supports LLDP packets from only nearest bridge agents.
- You can enable L2PT on a member port of a Layer 2 aggregation group, but the configuration does not take effect.
- LACP and EOAM require point-to-point transmission. If you enable L2PT for LACP or EOAM, L2PT multicasts LACP or EOAM packets out of customer-facing ports. As a result, the transmission between two CEs is not point-to-point. To ensure point-to-point transmission for the LACP or EOAM packets, you must configure other features (for example, VLAN).

Enabling L2PT for a protocol

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view: interface <i>interface-type interface-number</i> • Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-type</i> 	N/A

Step	Command	Remarks
	<i>interface-number</i>	
3. Enable L2PT for a protocol.	<ul style="list-style-type: none"> In Layer 2 Ethernet interface view: l2protocol { cdp dldp eoam gvrp lacp lldp mvrp pagp pvst stp vtp } tunnel dot1q In Layer 2 aggregate interface view: l2protocol { gvrp mvrp pvst stp vtp } tunnel dot1q 	By default, L2PT is disabled for all protocols.

Setting the destination multicast MAC address for tunneled packets

When you set the destination multicast MAC address for tunneled packets, follow these restrictions and guidelines:

- For tunneled packets to be recognized, set the same destination multicast MAC addresses on PEs that are connected to the same customer network.
- As a best practice, set different destination multicast MAC addresses on PEs connected to different customer networks. It prevents L2PT from sending packets of a customer network to another customer network.

To set the destination multicast MAC address for tunneled packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the destination multicast MAC address for tunneled packets.	l2protocol tunnel-dmac <i>mac-address</i>	The available multicast MAC addresses are 010f-e200-0003, 0100-0ccd-cdd0, 0100-0ccd-cdd1, and 0100-0ccd-cdd2. By default, 010f-e200-0003 is used for tunneled packets.

Displaying and maintaining L2PT

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

Task	Command
Display L2PT statistics.	display l2protocol statistics [interface <i>interface-type</i> <i>interface-number</i>]
Clear L2PT statistics.	reset l2protocol statistics [interface <i>interface-type</i> <i>interface-number</i>]

L2PT configuration examples

Configuring L2PT for STP

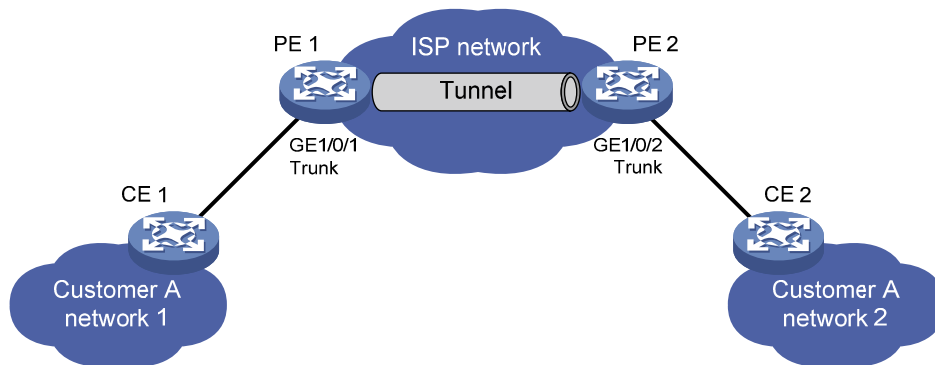
Network requirements

As shown in [Figure 33](#), the MAC addresses of CE 1 and CE 2 are 00e0-fc02-5800 and 00e0-fc02-5802, respectively. MSTP is enabled in Customer A's network, and default MSTP settings are used.

Perform the following tasks on the PEs:

- Configure the ports that connect to CEs as access ports, and configure the ports in the service provider network as trunk ports. Configure ports in the service provider network to allow packets from any VLAN to pass.
- Enable L2PT for STP to enable Customer A's network to implement independent spanning tree calculation across the service provider network.
- Set the destination multicast MAC address to 0100-0ccd-cdd0 for tunneled packets.

Figure 33 Network diagram



Configuration procedures

1. Configure PE 1:

Set the destination multicast address to 0100-0ccd-cdd0 for tunneled packets.

```
<PE1> system-view
[PE1] l2protocol tunnel-dmac 0100-0ccd-cdd0
```

Create VLAN 2.

```
[PE1] vlan 2
[PE1-vlan2] quit
```

Configure port GigabitEthernet 1/0/1 as an access port and assign the port to VLAN 2.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port access vlan 2
```

Disable STP and enable L2PT for STP on GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] undo stp enable
[PE1-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
[PE1-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet 1/0/2 connected to the service provider network as a trunk port, and assign the port to all VLANs.

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan all
```



```
[PE1-GigabitEthernet1/0/2] quit
```

2. Configure PE 2 in the same way PE 1 is configured. (Details not shown.)

Verifying the configuration

Verify that the root bridge of Customer A's network is CE 1.

```
<CE2> display stp root
```

MST ID	Root Bridge ID	ExtPathCost	IntPathCost	Root Port
0	32768.00e0-fc02-5800	0	0	

Verify that the root bridge of the service provider network is not CE 1.

```
[PE1] display stp root
```

MST ID	Root Bridge ID	ExtPathCost	IntPathCost	Root Port
0	32768.0cda-41c5-ba50	0	0	

Configuring L2PT for LACP

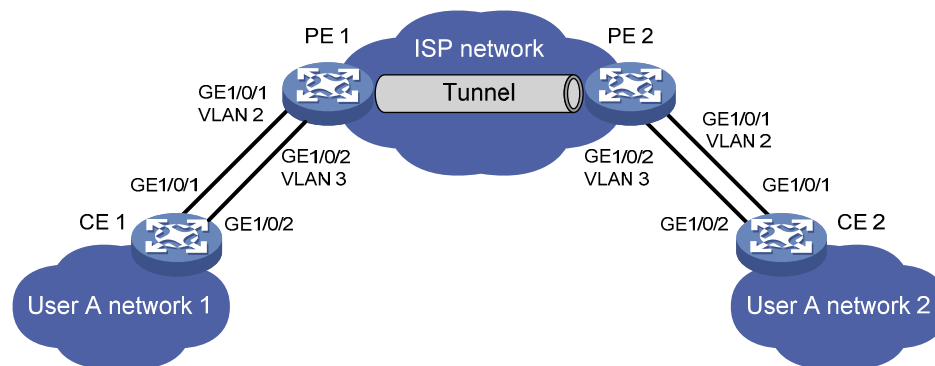
Network requirements

As shown in [Figure 34](#), the MAC addresses of CE 1 and CE 2 are 0001-0000-0000 and 0004-0000-0000, respectively.

Perform the following tasks:

- Configure Ethernet link aggregation on CE 1 and CE 2.
- Configure ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on CE 1 to form aggregate links with ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/2 on CE 2, respectively.
- Enable L2PT for LACP to enable CE 1 and CE 2 to implement Ethernet link aggregation across the service provider network.

Figure 34 Network diagram



Requirements analysis

To meet the network requirements, perform the following tasks:

- For Ethernet link aggregation to operate correctly, configure VLANs on the PEs to ensure point-to-point transmission between CE 1 and CE 2 in an aggregation group.
 - Set the PVIDs to VLAN 2 and VLAN 3 for ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on PE 1, respectively.
 - Configure PE 2 in the same way PE 1 is configured.
 - Configure ports that connect to the CEs as trunk ports.
- To retain the VLAN tag of the customer network, enable QinQ on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on both PE 1 and PE 2.

- For packets from any VLAN to be transmitted, configure all ports in the service provider network as trunk ports.

Configuration procedures

1. Configure CE 1:

Configure Layer 2 aggregation group Bridge-Aggregation 1 to operate in dynamic aggregation mode.

```
<CE1> system-view
[CE1] interface bridge-aggregation 1
[CE1-Bridge-Aggregation1] port link-type access
[CE1-Bridge-Aggregation1] link-aggregation mode dynamic
[CE1-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to Bridge-Aggregation 1.

```
[CE1] interface gigabitethernet 1/0/1
[CE1-GigabitEthernet1/0/1] port link-aggregation group 1
[CE1-GigabitEthernet1/0/1] quit
[CE1] interface gigabitethernet 1/0/2
[CE1-GigabitEthernet1/0/2] port link-aggregation group 1
[CE1-GigabitEthernet1/0/2] quit
```

2. Configure CE 2 in the same way CE 1 is configured. (Details not shown.)

3. Configure PE 1:

Create VLANs 2 and 3.

```
<PE1> system-view
[PE1] vlan 2
[PE1-vlan2] quit
[PE1] vlan 3
[PE1-vlan3] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, assign the port to VLAN 2, and set the PVID to VLAN 2.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-mode bridge
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 2
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 2
```

Enable QinQ on GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

Enable L2PT for LACP on GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] l2protocol lacp tunnel dot1q
[PE1-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, assign the port to VLAN 3, and set the PVID to VLAN 3.

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-mode bridge
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 3
[PE1-GigabitEthernet1/0/2] port trunk pvid vlan 3
```

Enable QinQ on GigabitEthernet 1/0/2.

```
[PE1-GigabitEthernet1/0/2] qinq enable
```

```
# Enable L2PT for LACP on GigabitEthernet 1/0/2.
```

```
[PE1-GigabitEthernet1/0/2] l2protocol lacp tunnel dot1q
[PE1-GigabitEthernet1/0/2] quit
```

4. Configure PE 2 in the same way PE 1 is configured. (Details not shown.)

Verifying the configuration

Verify that CE 1 and CE 2 have completed Ethernet link aggregation successfully.

```
[CE1] display link-aggregation member-port
```

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

```
GigabitEthernet1/0/1:
```

```
Aggregate Interface: Bridge-Aggregation1
```

```
Local:
```

```
Port Number: 3
Port Priority: 32768
Oper-Key: 1
Flag: {ACDEF}
```

```
Remote:
```

```
System ID: 0x8000, 0004-0000-0000
```

```
Port Number: 3
Port Priority: 32768
Oper-Key: 1
Flag: {ACDEF}
```

```
Received LACP Packets: 23 packet(s)
```

```
Illegal: 0 packet(s)
```

```
Sent LACP Packets: 26 packet(s)
```

```
GigabitEthernet1/0/2:
```

```
Aggregate Interface: Bridge-Aggregation1
```

```
Local:
```

```
Port Number: 4
Port Priority: 32768
Oper-Key: 1
Flag: {ACDEF}
```

```
Remote:
```

```
System ID: 0x8000, 0004-0000-0000
```

```
Port Number: 4
Port Priority: 32768
Oper-Key: 1
Flag: {ACDEF}
```

```
Received LACP Packets: 10 packet(s)
```

```
Illegal: 0 packet(s)
```

```
Sent LACP Packets: 13 packet(s)
```

```
[CE2] display link-aggregation member-port
```

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
 Port Number: 3
 Port Priority: 32768
 Oper-Key: 1
 Flag: {ACDEF}
Remote:
 System ID: 0x8000, 0001-0000-0000
 Port Number: 3
 Port Priority: 32768
 Oper-Key: 1
 Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
 Port Number: 4
 Port Priority: 32768
 Oper-Key: 1
 Flag: {ACDEF}
Remote:
 System ID: 0x8000, 0001-0000-0000
 Port Number: 4
 Port Priority: 32768
 Oper-Key: 1
 Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)

Configuring loop detection

Overview

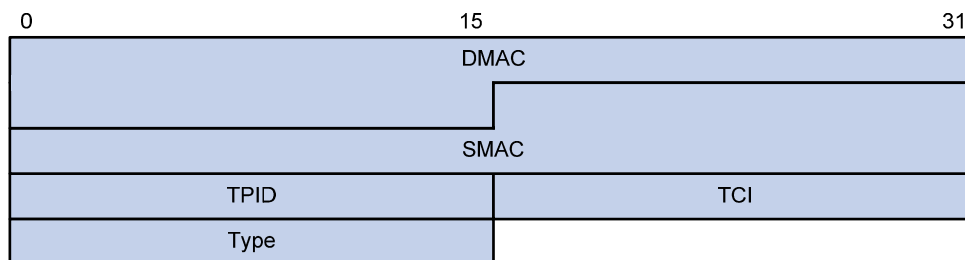
Incorrect network connections or configurations can create Layer 2 loops, which results in repeated transmission of broadcasts, multicasts, or unknown unicasts. The repeated transmission can waste network resources and can sometimes paralyze networks. The loop detection mechanism immediately generates 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](#)."

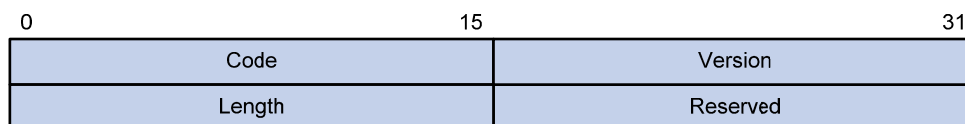
Figure 35 Ethernet frame header for loop detection



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 36 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 9 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

You can enable loop detection globally or on a per-port basis. The global configuration applies to all ports in the specified VLANs. The per-port configuration applies to the individual port only when the port belongs to the specified VLANs. Per-port configurations take precedence over global configurations.

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 { <i>vlan-list</i> 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable loop detection on the port.	loopback-detection enable vlan { <i>vlan-list</i> 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 <i>interface-type</i> <i>interface-number</i>	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 <i>interface-number</i>	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.

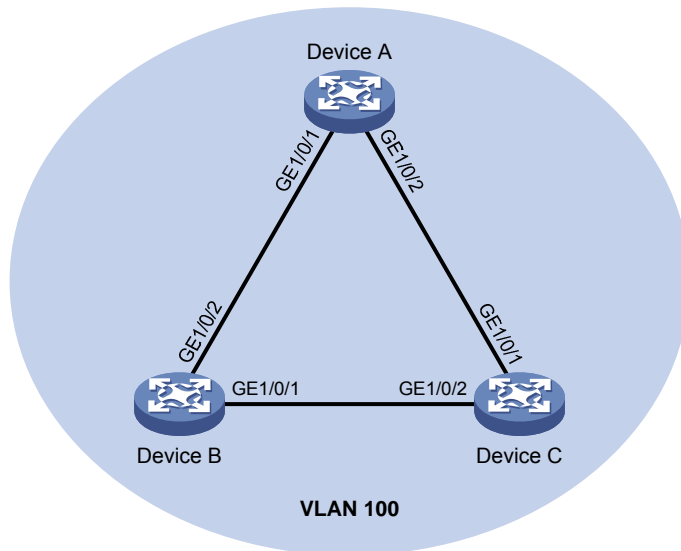
Task	Command
Display the loop detection configuration and status.	display loopback-detection

Loop detection configuration example

Network requirements

As shown in [Figure 37](#), 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 37 Network diagram



Configuration procedure

- 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 detects loops on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 within a loop detection interval.
- Device A automatically shuts down the ports and generates log messages.

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.

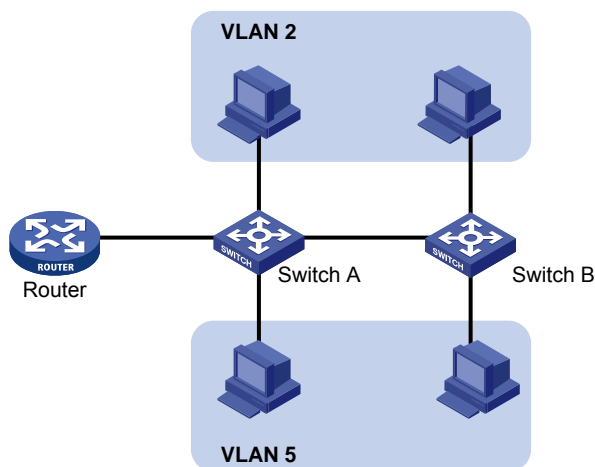
Configuring VLANs

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 38](#).

Figure 38 A VLAN diagram



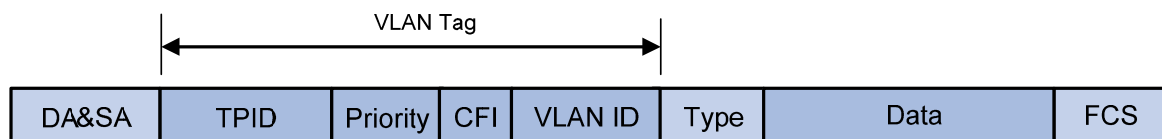
A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, you can assign all workstations and servers used by a particular workgroup to the same VLAN, regardless of their physical locations. Hosts in the same VLAN can directly communicate with one another. You 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 39 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. Possible values are:
 - **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 is VLAN tagged 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 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 { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }	By default, only the system default VLAN (VLAN 1) exists.
3. Enter VLAN view.	vlan <i>vlan-id</i>	To configure a VLAN after you create a list of VLANs, you must perform this step.
4. Configure a name for the VLAN.	name <i>text</i>	By default, the name of a VLAN is VLAN <i>vlan-id</i> . The <i>vlan-id</i> argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is VLAN 0100 .
5. Configure the description of the VLAN.	description <i>text</i>	By default, the description of a VLAN is VLAN <i>vlan-id</i> . The <i>vlan-id</i> argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is VLAN 0100 .

NOTE:

- As the system default VLAN, VLAN 1 cannot be created or removed.
 - You cannot use the **undo vlan** command to delete a dynamic VLAN, a VLAN configured with the QoS policy, or a VLAN locked by an application. To delete such a VLAN, first remove the configuration from the VLAN.
-

Configuring basic settings of a VLAN interface

For hosts of different VLANs to communicate at Layer 3, you can use VLAN interfaces. VLAN interfaces are virtual interfaces used for Layer 3 communication between different VLANs. They 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 are:
 - 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 <i>vlan-interface-id</i>	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 <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [sub]	By default, no IP address is assigned to any VLAN interface.
4. Configure the description of the VLAN interface.	description <i>text</i>	The default setting is the VLAN interface name. For example, Vlan-interface1 Interface.
5. Configure the MTU for the VLAN interface.	mtu <i>size</i>	The default setting is 1500 bytes.
6. Configure the expected bandwidth of the interface.	bandwidth <i>bandwidth-value</i>	By default, the expected bandwidth (in kbps) is the interface baud rate divided by 1000.
7. (Optional.) Restore the default settings for the VLAN interface.	default	N/A
8. (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. A hybrid port allows traffic from some VLANs to pass through untagged and traffic from other VLANs to pass through tagged. Hybrid ports are typically used in one-to-two VLAN mapping to remove SVLAN tags before forwarding packets from multiple service provider VLANs to the customer network. 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 remove 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 local and remote ports.
- Make sure a port is assigned to its PVID. Otherwise, when the port receives frames tagged with the PVID or untagged frames, the port filters out these frames.

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.	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Receives the frame if its VLAN ID is the same as the PVID.• Drops the frame if its VLAN ID is	<ul style="list-style-type: none">• 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
	different from the PVID.		
In the outbound direction	Removes the VLAN tag and sends the frame.	<ul style="list-style-type: none"> 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 <i>vlan-id</i>	N/A
3. Assign one or multiple access ports to the VLAN.	port <i>interface-list</i>	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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	<ul style="list-style-type: none"> 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

Step	Command	Remarks
		aggregation member ports.
3. Set the port link type to access.	port link-type access	By default, all ports are access ports.
4. (Optional.) Assign the access port to a VLAN.	port access vlan <i>vlan-id</i>	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.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view: interface <i>interface-type interface-number</i> • Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	<ul style="list-style-type: none"> • 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. Set the port link type to 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 { <i>vlan-id-list</i> all }	By default, a trunk port only permits VLAN 1.
5. (Optional.) Configure the PVID of the trunk port.	port trunk pvid vlan <i>vlan-id</i>	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.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> • Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	<ul style="list-style-type: none"> • 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. Set the port link type to hybrid.	port link-type hybrid	By default, all ports are access ports.
4. Assign the hybrid port to the specified VLANs.	port hybrid vlan <i>vlan-id-list</i> { 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 <i>vlan-id</i>	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, you must 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.

After the static MAC-based VLAN assignment is configured, the port processes a received frame as follows:

- For an untagged frame, the port determines the VLAN ID for it in the following workflow:
 - a. The port first performs a fuzzy match. The port searches for the MAC-to-VLAN entries whose masks are not all-Fs and 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 and forwards the frame.
 - b. If the fuzzy match fails, the port performs an exact match by searching for the 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 and forwards the frame.
 - c. If no matching VLAN ID is found, other criteria, such as IP subnet or protocol, are used for VLAN assignment before the frame is forwarded.
 - d. If no VLAN is available, the port tags the frame with its PVID and forwards the frame.
- For a tagged frame, the port processes it as follows:
 - 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 do that, you must 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.

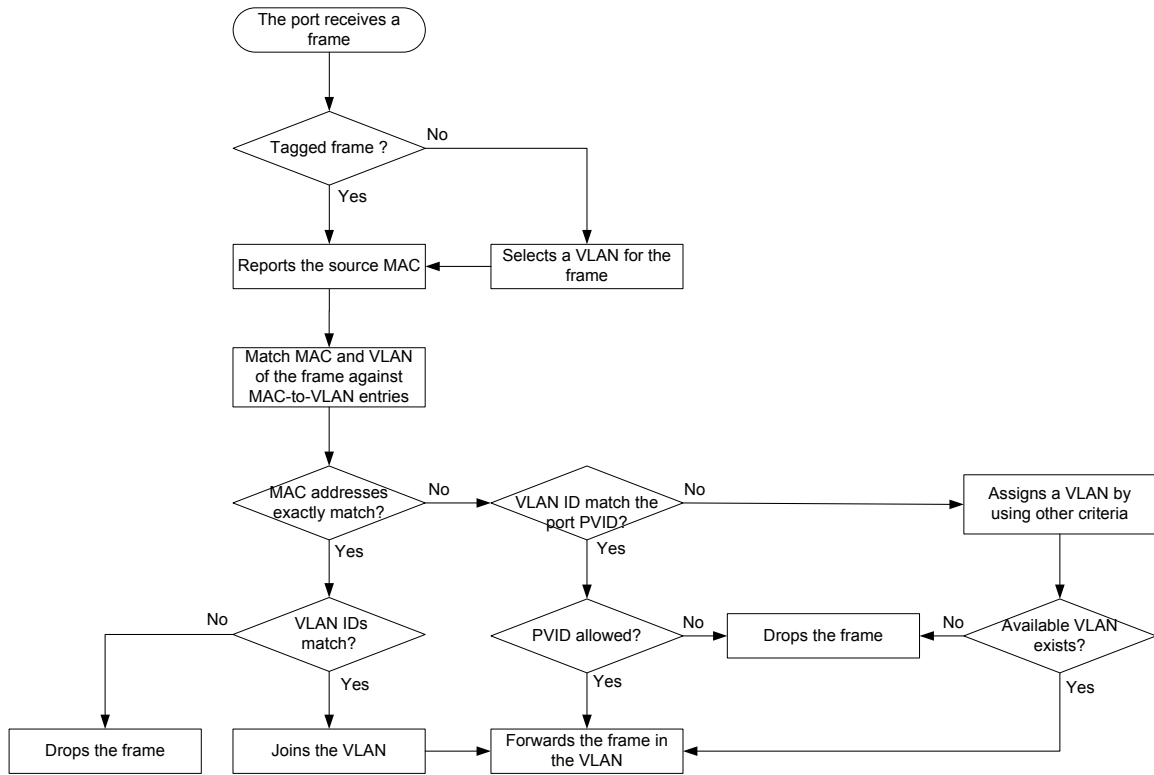
Dynamic MAC-based VLAN assignment uses the following workflow, as shown in [Figure 40](#):

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 examines the VLAN ID of the frame as follows:
 - 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 40 Flowchart for processing a frame in dynamic MAC-based VLAN assignment



When you configure dynamic MAC-based VLAN assignment, follow these guidelines:

- A port joins a VLAN specified in the MAC-to-VLAN entry as an untagged member if the port has not been configured to allow packets from the VLAN to pass through.
- 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 tasks:

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 disable 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 static and 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 <i>interface-number</i>	N/A
4. Set the port link type to 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.
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 <i>mac-address</i> vlan <i>vlan-id</i> [dot1q <i>priority</i>]	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 <i>interface-type</i> <i>interface-number</i>	N/A
4. Set the port link type to 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. As a best practice to ensure the priority of MAC-based VLAN matching, configure the vlan precedence mac-vlan command when you enable dynamic MAC-based VLAN assignment. 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
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the port link type to 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 <i>vlan-id-list</i> { tagged untagged }	By default, a hybrid port is an untagged member of the VLAN to which the port belongs when

Step	Command	Remarks
		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 <i>Security Command Reference</i> .	N/A

Configuring IP subnet-based VLANs

Introduction

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.

Configuration procedure

To configure a IP subnet-based VLAN:

Task	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Associate an IP subnet or IP address with the VLAN.	ip-subnet-vlan [<i>ip-subnet-index</i>] ip <i>ip-address</i> [<i>mask</i>]	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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	<ul style="list-style-type: none"> 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 the aggregate interface. If the system fails to apply the configurations to an aggregation member port, it skips the port and moves to the next member port.

Task	Command	Remarks
6. Set the port link type to hybrid.	port link-type hybrid	By default, all ports are access ports.
7. Configure the hybrid port to forward packets from the specified IP subnet-based VLANs.	port hybrid vlan <i>vlan-id-list</i> { 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 <i>vlan-id</i>	By default, no IP subnet-based VLAN is associated with a hybrid port.

Configuring protocol-based VLANs

Introduction

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, you must 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.

Configuration procedure

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 <i>vlan-id</i>	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 [<i>protocol-index</i>] { at ipv4 ipv6 ipx { ethernetii llc snap } mode { ethernetii etertype <i>etype-id</i> llc { dsap <i>dsap-id</i> [ssap <i>ssap-id</i>] ssap <i>ssap-id</i> } snap etertype <i>etype-id</i> }	By default, no protocol template is configured for a VLAN.
4. Exit VLAN view.	quit	N/A
5. Enter interface view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	<ul style="list-style-type: none"> 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. Set the port link type to 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 <i>vlan-id-list</i> { 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 <i>vlan-id</i> { <i>protocol-index</i> [to <i>protocol-end</i>] all }	By default, a port is not associated with any protocol-based VLANs.

Configuring a VLAN group

A VLAN group includes a set of VLANs.

On an authentication server, a VLAN group name represents a group of authorization VLANs. When an 802.1X user passes authentication, the authentication server assigns a VLAN group name to the device. The device then uses the received VLAN group name to match the locally configured VLAN group names. If a match is found, the device selects a VLAN from the group and assigns the VLAN to the user. 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 <i>group-name</i>	By default, no VLAN group exists.
3. Add VLANs to the VLAN	vlan-list <i>vlan-id-list</i>	By default, no VLAN exists in a

Step	Command	Remarks
group.		VLAN group. You can add multiple VLAN lists to a VLAN group.

Displaying and maintaining VLANs

Execute **display** commands in any view.

Task	Command
Display VLAN interface information.	display interface vlan-interface [brief [down description]] display interface vlan-interface [<i>interface-number</i>] [brief [description]]
Display MAC-to-VLAN entries.	display mac-vlan { all dynamic mac-address <i>mac-address</i> [mask <i>mac-mask</i>] static vlan <i>vlan-id</i> }
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 { <i>interface-type interface-number1</i> [to <i>interface-type interface-number2</i>] all }
Display information about IP subnet-based VLANs.	display ip-subnet-vlan vlan { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }
Display information about protocol-based VLANs that are associated with the specified ports.	display protocol-vlan interface { <i>interface-type interface-number1</i> [to <i>interface-type interface-number2</i>] all }
Display information about protocol-based VLANs.	display protocol-vlan vlan { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }
Display VLAN information.	display vlan [<i>vlan-id1</i> [to <i>vlan-id2</i>] all dynamic reserved static]
Display brief VLAN information.	display vlan brief
Display VLAN group information.	display vlan-group [<i>group-name</i>]
Display hybrid ports or trunk ports on the device.	display port { hybrid trunk }

VLAN configuration examples

Port-based VLAN configuration example

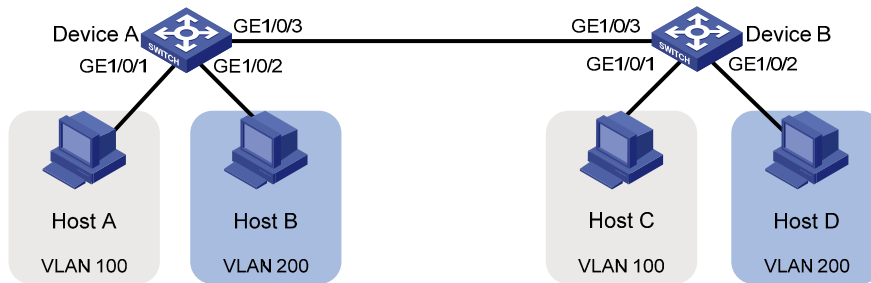
Network requirements

As shown in [Figure 41](#):

- 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 41 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

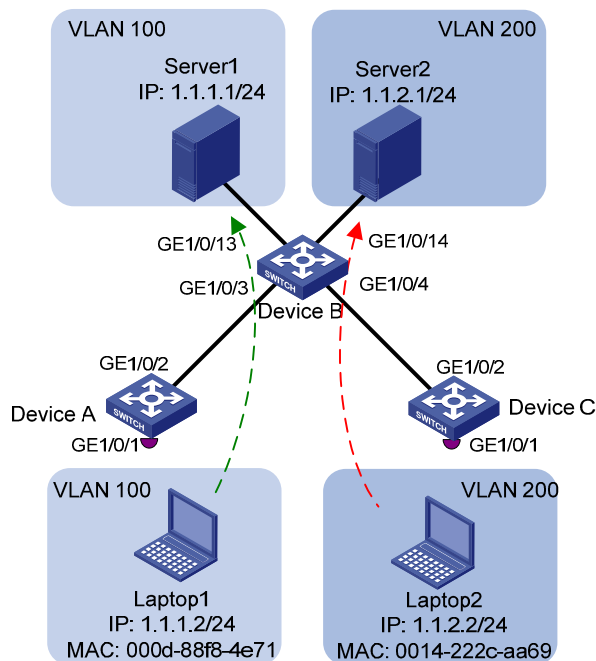
Network requirements

As shown in [Figure 42](#):

- 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 it is used in.

Figure 42 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

1. Verify that Laptop 1 can access only Server 1, and Laptop 2 can access only Server 2. (Details not shown.)

2. 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:

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

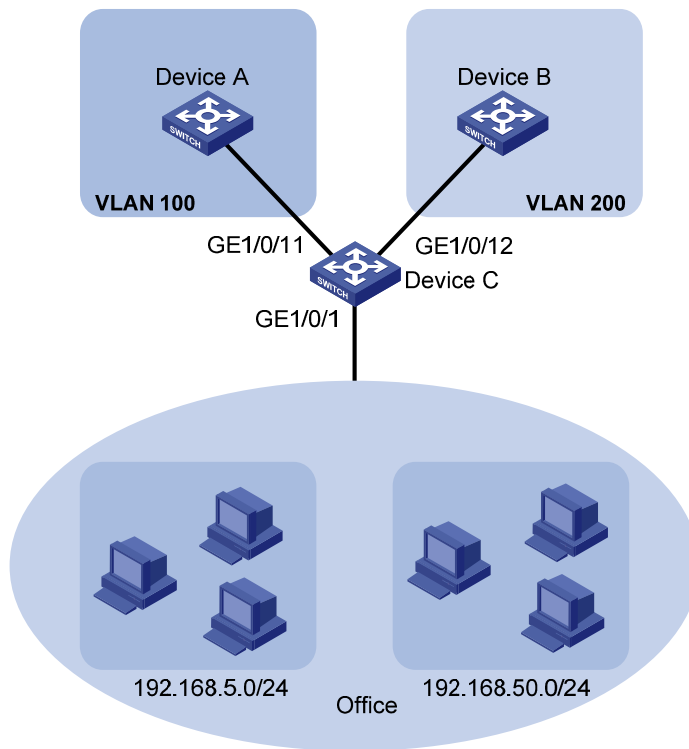
IP subnet-based VLAN configuration example

Network requirements

As shown in [Figure 43](#), 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 43 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 to forward packets from VLAN 100 to pass through with VLAN tags.

```
[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 to forward packets from VLAN 200 to pass through with VLAN tags.

```
[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 to forward packets from VLANs 100 and 200 without VLAN tags.

```
[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

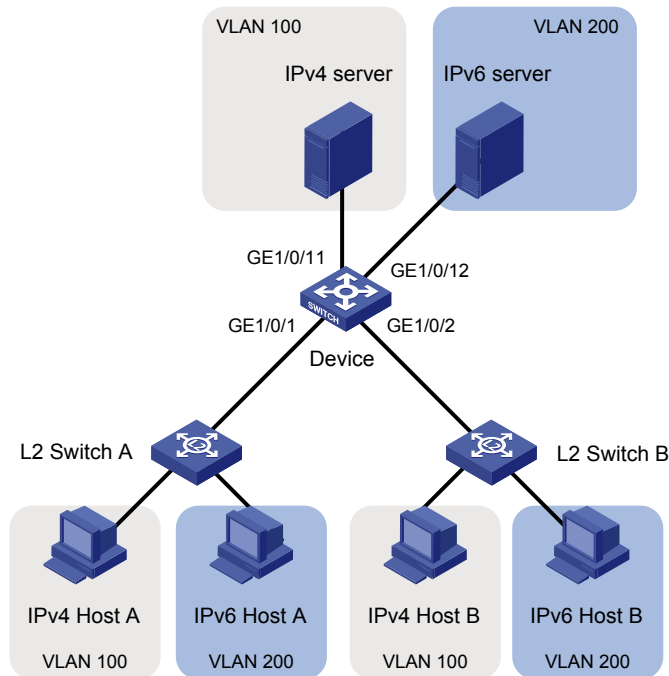
Network requirements

As shown in [Figure 44](#):

- 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 44 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 to forward packets from VLANs 100 and 200 without VLAN tags.

```
[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 to forward packets from VLANs 100 and 200 without VLAN tags.

```
[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:

- o The hosts and the server in VLAN 100 can successfully ping one another. (Details not shown.)
- o The hosts and the server in VLAN 200 can successfully ping one another. (Details not shown.)
- o 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 the VLAN interface. 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:
 - o 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.
 - o 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 <i>vlan-id</i>	By default, only the 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 <i>vlan-id</i>	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 <i>vlan-id-list</i>	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

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 <i>vlan-interface</i> <i>vlan-interface-id</i>	The <i>vlan-interface-id</i> argument must be the super VLAN ID.
3. Configure an IP address for the VLAN interface of the super VLAN.	<ul style="list-style-type: none"> Configure an IPv4 address: ip address <i>ip-address</i> { <i>mask-length</i> <i>mask</i> } [sub] Configure an IPv6 address: ipv6 address { <i>ipv6-address</i> <i>prefix-length</i> <i>ipv6-address/prefix-length</i> } 	By default, no IP address is configured for a VLAN interface.
4. (Optional.) Configure Layer 3 communication between sub VLANs.	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 <i>Layer 3—IP Services Configuration Guide</i> . For more information about local-proxy-arp enable and local-proxy-nd enable commands, see <i>Layer 3—IP Services Command Reference</i> .

Displaying and maintaining super VLANs

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

Task	Command
Display information about super VLANs and all sub VLANs associated with each super VLAN.	display supervlan [<i>supervlan-id</i>]

Super VLAN configuration example

Network requirements

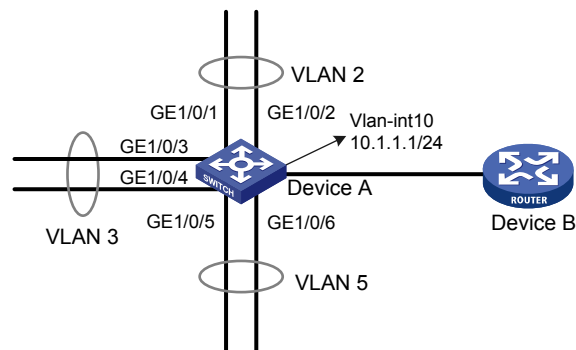
As shown in [Figure 45](#):

- 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 45 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 VLAN 2, VLAN 3, and VLAN 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

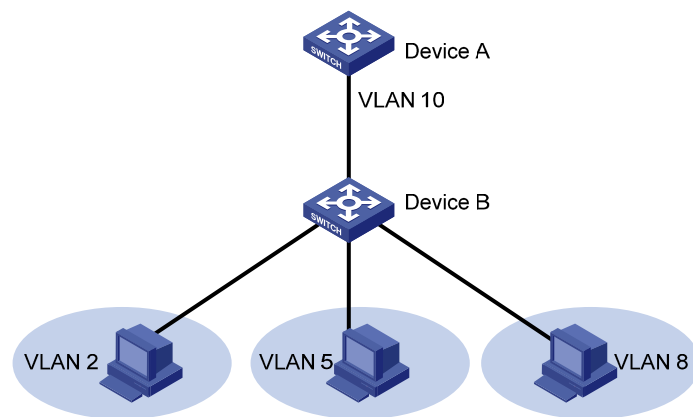
The private VLAN feature uses a two-tier VLAN structure, including a primary VLAN and secondary VLANs. This feature simplifies the network configuration and saves VLAN resources.

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 46](#)).

As shown in [Figure 46](#), 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 46 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:
 - o Configure the uplink port (for example, the port connecting Device B to Device A in [Figure 46](#)):
 - 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.
 - o Configure a downlink port (for example, the port connecting Device B to a host in [Figure 46](#)) as a host port. The host port can be automatically assigned to the secondary VLAN and its associated primary VLAN.
 - o 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 <i>vlan-id</i>	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 { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }	N/A
6. Enable Layer 2 communication for ports in the same secondary VLAN.	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <i>interface-type</i> <i>interface-number</i>	N/A
9. Configure the uplink port as a promiscuous or trunk promiscuous port of the specified VLANs.	<ul style="list-style-type: none"> Configure the uplink port as a promiscuous port of the specified VLAN: port private-vlan <i>vlan-id</i> promiscuous Configure the uplink port as a trunk promiscuous port of the specified VLANs: port private-vlan <i>vlan-id-list</i> 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 <i>interface-type</i> <i>interface-number</i>	N/A
12. Assign the downlink port to secondary VLANs.	<ol style="list-style-type: none"> Set the link type of the port: port link-type { access hybrid trunk } Assign the access port to the specified VLAN: port access vlan <i>vlan-id</i> Assign the trunk port to the specified VLANs: port trunk permit vlan { <i>vlan-id-list</i> all } Assign the hybrid port to the specified VLANs: port hybrid vlan <i>vlan-id-list</i> { 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 <i>interface-type</i> <i>interface-number</i>	N/A
15. Configure the downlink port as a host or trunk secondary port.	<ul style="list-style-type: none"> Configure the downlink port as a host port: port private-vlan host Configure the downlink port as a trunk secondary port: port private-vlan <i>vlan-id-list</i> trunk secondary 	By default, a port is not a host or trunk secondary port.
16. Enter primary VLAN view.	vlan <i>vlan-id</i>	N/A
17. Associate the primary VLAN with the specified secondary VLANs.	private-vlan secondary <i>vlan-id-list</i>	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.	<p>a. Enter VLAN interface view of the primary VLAN interface: interface vlan-interface <i>vlan-id</i></p> <p>b. Enable Layer 3 communication between secondary VLANs that are associated with the primary VLAN: private-vlan secondary <i>vlan-id-list</i></p> <p>c. Assign an IPv4 address to the primary VLAN interface: ip address <i>ip-address</i> { <i>mask-length</i> <i>mask</i> } [<i>sub</i>]</p> <p>d. Assign an IPv6 address to the primary VLAN interface: ipv6 address { <i>ipv6-address</i> <i>prefix-length</i> <i>ipv6-address/prefix-length</i> <i>h</i> }</p> <p>e. Enable local proxy ARP: local-proxy-arp enable</p> <p>f. Enable local proxy ND: local-proxy-nd enable</p>	<p>Use substeps a, b, c, and e for devices that run IPv4 protocols.</p> <p>Use substeps a, b, d, and f for devices that run IPv6 protocols.</p> <p>By default:</p> <ul style="list-style-type: none"> 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 the **display** command in any view.

Task	Command
Display information about primary VLANs and the secondary VLANs associated with each primary VLAN.	display private-vlan [<i>primary-vlan-id</i>]

Private VLAN configuration examples

Promiscuous port configuration example

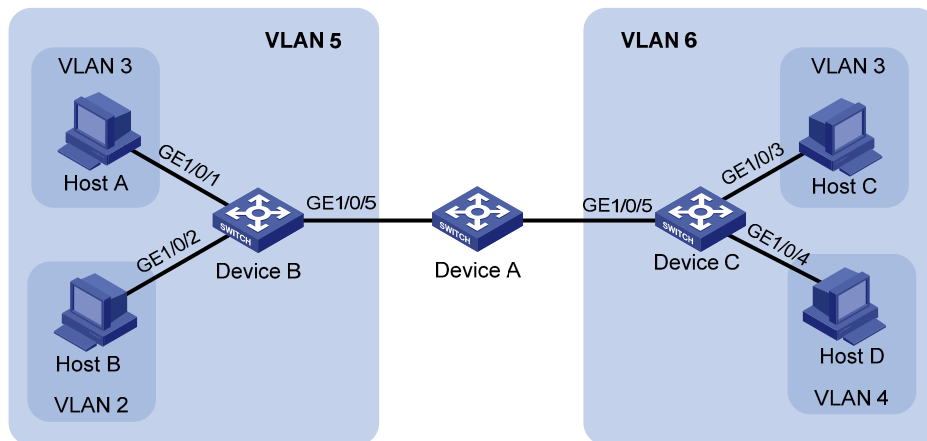
Network requirements

As shown in [Figure 47](#), 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 47 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.

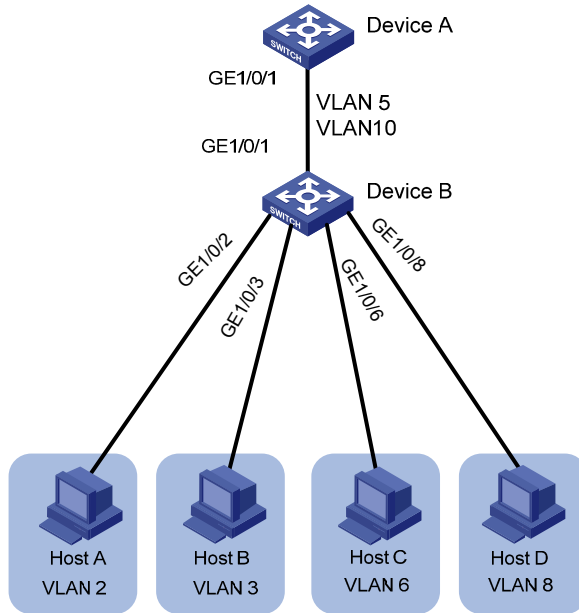
Trunk promiscuous port configuration example

Network requirements

As shown in [Figure 48](#), configure the private VLAN feature to meet the following requirements:

- VLAN 5 and VLAN 10 are primary VLANs on Device B. The uplink port GigabitEthernet 1/0/1 permits the packets from VLAN 5 and VLAN 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 48 Network diagram



Configuration procedure

1. Configure Device B:

Configure VLAN 5 and VLAN 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 VLAN 5 and VLAN 10.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and configure the port to permit packets from VLAN 5 and VLAN 10 to pass through tagged.

```
[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

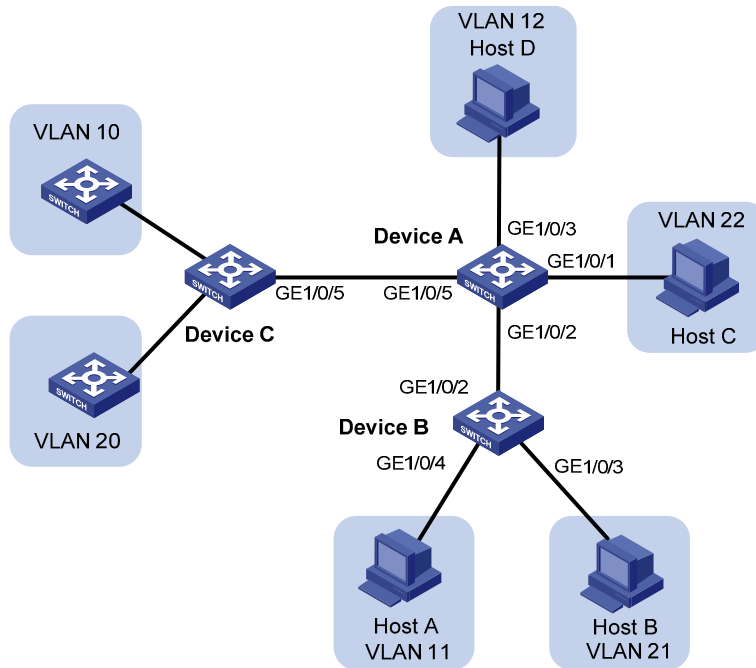
Network requirements

As shown in [Figure 49](#), configure the private VLAN feature to meet the following requirements:

- VLAN 10 and VLAN 20 are primary VLANs on Device A. The uplink port GigabitEthernet 1/0/5 permits the packets from VLAN 10 and VLAN 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 49 Network diagram



Configuration procedure

1. Configure Device A:

Configure VLAN 10 and VLAN 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 VLAN 10 and VLAN 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 VLAN 11 and VLAN 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 VLAN 11 and VLAN 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 configure the port to permit packets from VLAN 11 and VLAN 21 to pass through tagged.

```
[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 VLAN 10 and VLAN 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 configure the port to permit packets from VLAN 10 and VLAN 20 to pass through tagged.

```
[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.

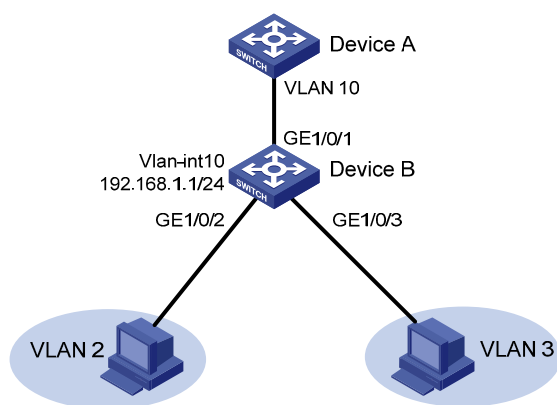
Secondary VLAN Layer 3 communication configuration example

Network requirements

As shown in [Figure 50](#), 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 50 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.

```
[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 the IP phone as an example.

For the voice traffic transmission, the device must perform the following tasks:

- 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 out of 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 10](#)) or configure OUI addresses for the device. You can manually remove or add the system default OUI addresses.

The switch supports 16 OUI addresses, including system default OUI addresses.

Table 10 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 logic AND results of the *mac-address* and *oui-mask* arguments in the **voice-vlan mac-address** command.

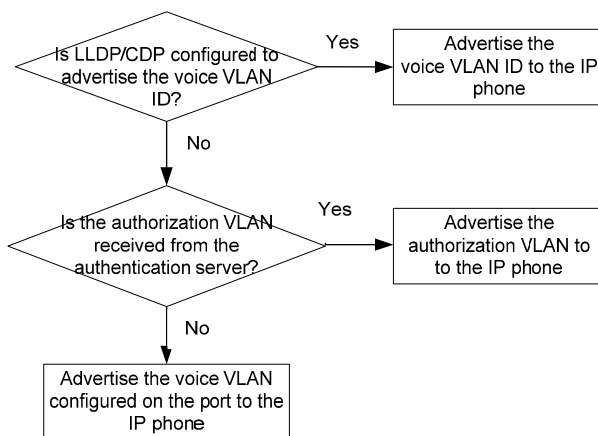
Automatically identifying IP phones through LLDP

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 51 shows the workflow of advertising the voice VLAN information to IP phones.

Figure 51 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."](#)

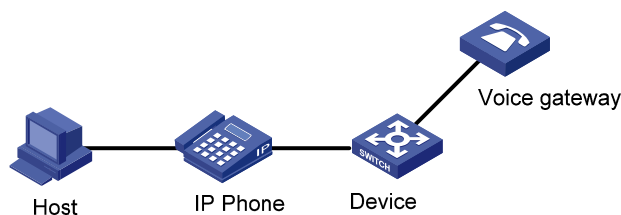
IP phone access methods

Connecting the host and the IP phone in series

As shown in [Figure 52](#), 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.

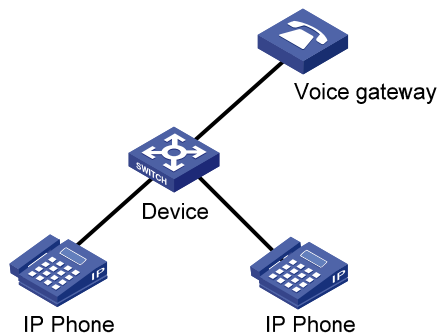
Figure 52 Connecting the host and IP phone in series



Connecting the IP phone to the device

As shown in [Figure 53](#), 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 53 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 52](#). Ports on the device transmit both voice traffic and data traffic.

When an IP phone is powered on, it sends out protocol packets. The system matches the source MAC address of the protocol packets against the device's OUI addresses. If the match succeeds, the system performs the following tasks:

- 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. Voice traffic triggering is not required 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 53](#). In this mode, ports assigned to a voice VLAN transmit voice traffic exclusively, which prevents the data traffic impact on the voice traffic transmission.

You must manually assign the receiving port on the device to a voice VLAN. The system matches the source MAC address in the packets against the device's 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 process, ports of different link types must meet specific configuration requirements in different voice VLAN assignment modes.

Table 11 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 12 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 receives only voice packets whose source MAC addresses match the OUI addresses. All other packets are 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 13 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	<ul style="list-style-type: none"> 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 include the CoS and DSCP values. Voice traffic carries its own QoS priority settings. 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure QoS priority settings for incoming voice VLAN packets.	<ul style="list-style-type: none"> • Configure the port to trust the QoS priority settings: voice-vlan qos trust • Configure the port to modify the CoS and DSCP values: voice-vlan qos <i>cos-value</i> <i>dscp-value</i> 	<p>By default, a port modifies the CoS and DSCP values for voice VLAN packets to 6 and 46, respectively.</p> <p>If a port trusts the QoS priority settings in incoming voice VLAN packets, the port does not modify their CoS and DSCP values.</p> <p>If you execute the voice-vlan qos and voice-vlan qos trust commands multiple times, the most recent configuration takes effect.</p>

Configuring a port to operate in automatic 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 <i>minutes</i>	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 <i>oui mask oui-mask [description text]</i>	By default, system default OUI addresses exist. For more information, see Table 10 .
5. Enter Layer 2 Ethernet interface view.	interface <i>interface-type interface-number</i>	N/A
6. Configure the link type of the port.	<ul style="list-style-type: none"> • 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 <i>vlan-id enable</i>	By default, the voice VLAN feature is disabled.

Configuring a port to operate in manual 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. However, you can configure one port with only one voice VLAN, and this voice VLAN must be a static VLAN that already exists on the device.
- 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 <i>oui</i> mask <i>oui-mask</i> [description <i>text</i>]	By default, system default OUI addresses exist. For more information, see Table 10 .
4. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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 <i>vlan-id</i> 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 function only with the automatic voice VLAN assignment mode.
- You cannot use this function 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 51](#).

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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure LLDP or CDP to advertise a voice VLAN.	<ul style="list-style-type: none"> • Configure LLDP to advertise a voice VLAN: lldp tlv-enable med-tlv network-policy <i>vlan-id</i> • Configure CDP to advertise a voice VLAN: <ol style="list-style-type: none"> a. Specify the ID of an advertised VLAN: cdp voice-vlan <i>vlan-id</i> b. Configure CDP compatibility: For more information, see "Configuring LLDP." 	<p>By default, LLDP and CDP advertise the voice VLAN configured on the port.</p> <p>For more information about the lldp tlv-enable med-tlv network-policy command, see Layer 2—LAN Switching Command Reference.</p>
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

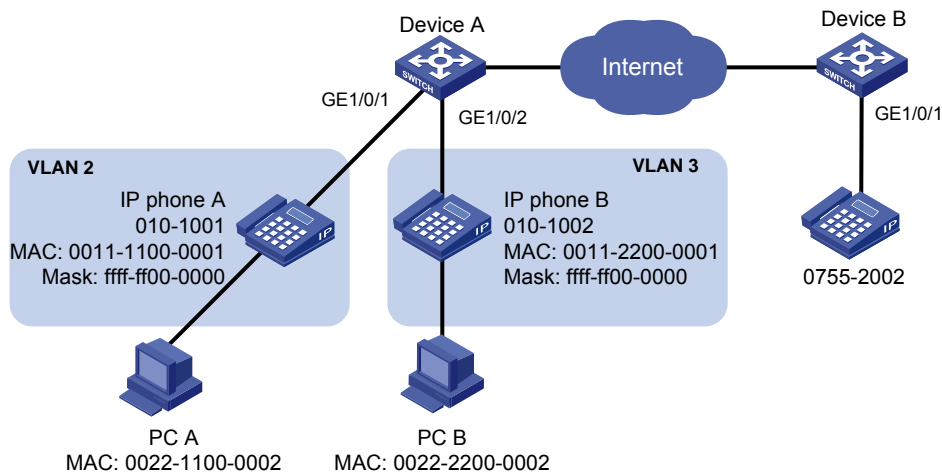
Network requirements

As shown in Figure 54, 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 54 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	
0011-1100-0000	ffff-ff00-0000	IP phone A	
0011-2200-0000	ffff-ff00-0000	IP phone B	
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	
000f-e200-0000	ffff-ff00-0000	H3C Aolynk 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
GE1/0/1	2	AUTO	6	46
GE1/0/2	3	AUTO	6	46

Manual voice VLAN assignment mode configuration example

Network requirements

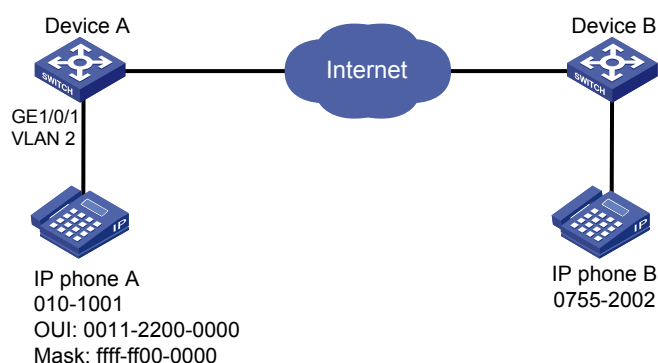
As shown in [Figure 55](#):

- 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 55 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 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
0011-2200-0000   ffff-ff00-0000   test
00d0-1e00-0000   ffff-ff00-0000   Pingtel phone
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
00e0-7500-0000   ffff-ff00-0000   Polycom phone
00e0-bb00-0000   ffff-ff00-0000   3com phone
000f-e200-0000   ffff-ff00-0000   H3C Aolynk 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
GE1/0/1           2         Manual    6         46
```

Configuring MVRP

Multiple Registration Protocol (MRP) is an attribute registration protocol used to transmit attribute messages.

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

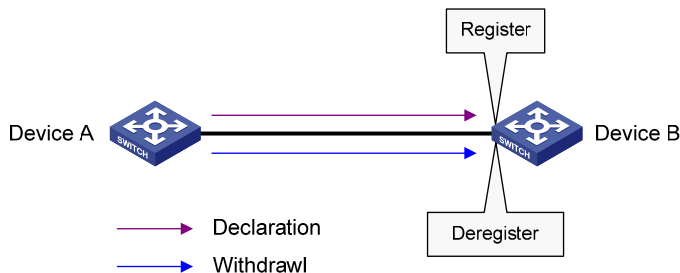
MRP allows devices in the same LAN to transmit attribute messages on a per MSTI basis. For more information about MSTI, see "[Configuring spanning tree protocols.](#)"

MRP implementation

Each port that participates in an MRP application is called an MRP participant. A port that participates in an MVRP application is called an MVRP participant.

As shown in [Figure 56](#), an MRP participant registers and deregisters its attribute values on other MRP participants by sending declarations and withdrawals. It also registers and deregisters the attribute values of other participants according to received declarations and withdrawals. MRP rapidly propagates the configuration information of an MRP participant throughout the LAN.

Figure 56 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 56](#) 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 Join, New, Leave, and LeaveAll. Join and New messages are declarations, and Leave and LeaveAll messages are withdrawals.

Join message

An MRP participant sends a Join message to request the peer participant to register attributes.

When receiving a Join message from the peer participant, an MRP participant performs the following tasks:

- Registers the attributes.
- Propagates the Join message to all other participants on the device.

After receiving this message, a participant sends a Join message to its peer participants.

Join messages sent from a local device to a peer device include the following types:

- **JoinEmpty**—Declares an unregistered attribute. For example, an MRP participant joins an existing static VLAN and sends a Join message before registering the VLAN. The Join message is a JoinEmpty message. VLANs created manually and locally are called static VLANs, and 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

MRP sends a Leave message to the peer participant to deregister attributes that an MRP participant has deregistered.

When the local MRP participant receives a Leave message from the peer participant, it performs the following tasks:

- Deregisters the attribute.
- Propagates the Leave message to other participants on the device.

After receiving the Leave message, a participant determines whether to send the Leave message to its peer participants depending on the attribute status on the device. For example, if a Leave message is received for a dynamic VLAN not registered by any participant on the device, both of the following events occur:

- The VLAN is deleted on the device.
- The Leave message is sent to the peer participants.

If a Leave message for a static VLAN is received, the Leave message will not be sent to the peer participants.

LeaveAll message

Each MRP participant is configured with an individual LeaveAll timer. 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. MRP

re-registers the attributes in the received Join message before the Leave timer expires. When the Leave timer expires, MRP 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, it sends stored MRP messages in as few packets as possible and restarts the Periodic timer. This mechanism reduces the number of MRP packets periodically sent.

You can enable or disable the Periodic timer at the CLI. If you disable the Periodic timer, MRP does not periodically send MRP messages. Instead, MRP sends MRP messages when the LeaveAll timer expires or it 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 another 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. Upon receiving a Leave message, MRP starts the Leave timer. If it receives a Join message for the attributes in the Leave message before the Leave timer expires, MRP does not deregister the attributes. In addition, when an MRP participant sends or receives a LeaveAll message, it starts the Leave timer. If it receives a Join message for some attributes in the LeaveAll message before the Leave timer expires, MRP does not deregister the attributes. Otherwise, MRP deregisters the attributes.

LeaveAll timer

After startup, an MRP participant starts its own LeaveAll timer. When the LeaveAll timer expires, MRP sends out a LeaveAll message and restarts the LeaveAll timer. After receiving the LeaveAll message, other participants restart their LeaveAll timer.

When its LeaveAll timer expires, an MRP participant sends a LeaveAll message to other participants. Upon receiving a LeaveAll message, a participant restarts its LeaveAll timer, and stops sending out LeaveAll messages. This mechanism effectively reduces the number of LeaveAll messages in the network.

The system randomly changes the LeaveAll timer within a certain range for an MRP participant when the participant restarts its LeaveAll timer. This 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 static and dynamic VLANs in different ways.

Normal

An MVRP participant in normal registration mode performs dynamic VLAN registrations and deregistrations.

Fixed

An MVRP participant in fixed registration mode disables deregistering dynamic VLANs and drops received MVRP packets. The MVRP participant does not deregister or register dynamic VLANs.

Forbidden

An MVRP participant in forbidden registration mode disables registering dynamic VLANs and drops received MVRP packets. The MVRP participant does not register dynamic VLANs, or re-register a dynamic VLAN when the VLAN is deregistered.

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.) Configuring an MVRP registration mode
(Optional.) Configuring 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. However, MVRP cannot work with other link layer topology protocols, including PVST, and Smart Link. Ports blocked by STP, RSTP, or MSTP can receive and send MVRP protocol packets. For more information about STP, RSTP, MSTP, and PVST, see "[Configuring spanning tree protocols](#)."
- Do not enable both MVRP and remote port mirroring on a port. Otherwise, MVRP might register the remote probe VLAN to incorrect ports, which would cause the monitor port to receive undesired duplicates. For more information about port mirroring, see *Network Management and Monitoring Configuration Guide*.
- 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 a member port in an aggregation group takes effect only after the port is removed from the aggregation group.

Configuration prerequisites

Before configuring MVRP, perform the following tasks:

- Because MVRP runs on a per-MSTI basis, make sure the following requirements are met:
 - All MSTIs in the network are effective.

- Each MSTI is mapped to an existing VLAN on each device in the network.
- Configure the involved ports as trunk ports, because MVRP takes effect only on trunk ports. For more information about trunk ports, see "Configuring VLANs."

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 <i>interface-type</i> <i>interface-number</i>	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 <i>Layer 2—LAN Switching Command Reference</i> .
5. Configure the trunk port to permit the specified VLANs.	port trunk permit vlan { <i>vlan-id-list</i> 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 <i>Layer 2—LAN Switching Command Reference</i> .
6. Enable MVRP on the port.	mvrp enable	By default, MVRP is disabled on a port.

Configuring 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an MVRP registration mode.	mvrp registration { fixed forbidden normal }	Optional. The default setting is normal registration mode.

Configuring 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 configure 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 <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the LeaveAll timer.	mrp timer leaveall <i>timer-value</i>	Optional. The default setting is 1000 centiseconds.
4. Configure the Join timer.	mrp timer join <i>timer-value</i>	Optional. The default setting is 20 centiseconds.
5. Configure the Leave timer.	mrp timer leave <i>timer-value</i>	Optional. The default setting is 60 centiseconds.
6. Configure the Periodic timer.	mrp timer periodic <i>timer-value</i>	Optional. The default setting is 100 centiseconds. You can restore the Periodic timer to the default at any time.

Table 14 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 14.
- As a best practice, restore the timers in the order of Join, Leave, and LeaveAll.

Table 14 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, so that the local end can receive and send both MVRP and GVRP packets. For more information about GVRP, see relevant protocols and standards.

GVRP compatibility enables MVRP to work with STP or RSTP, but not MSTP. When MVRP with GVRP compatibility enabled works with MSTP, the network might operate incorrectly.

Disable the Period timer when you enable GVRP compatibility for MVRP. Otherwise, the VLAN status might frequently change when the system is busy.

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 <i>interface-list</i>]
Display the MVRP state of a port in a VLAN.	display mvrp state interface <i>interface-type interface-number</i> vlan <i>vlan-id</i>
Display MVRP statistics.	display mvrp statistics [interface <i>interface-list</i>]
Clear MVRP statistics.	reset mvrp statistics [interface <i>interface-list</i>]

MVRP configuration example

Network requirements

As shown in [Figure 57](#):

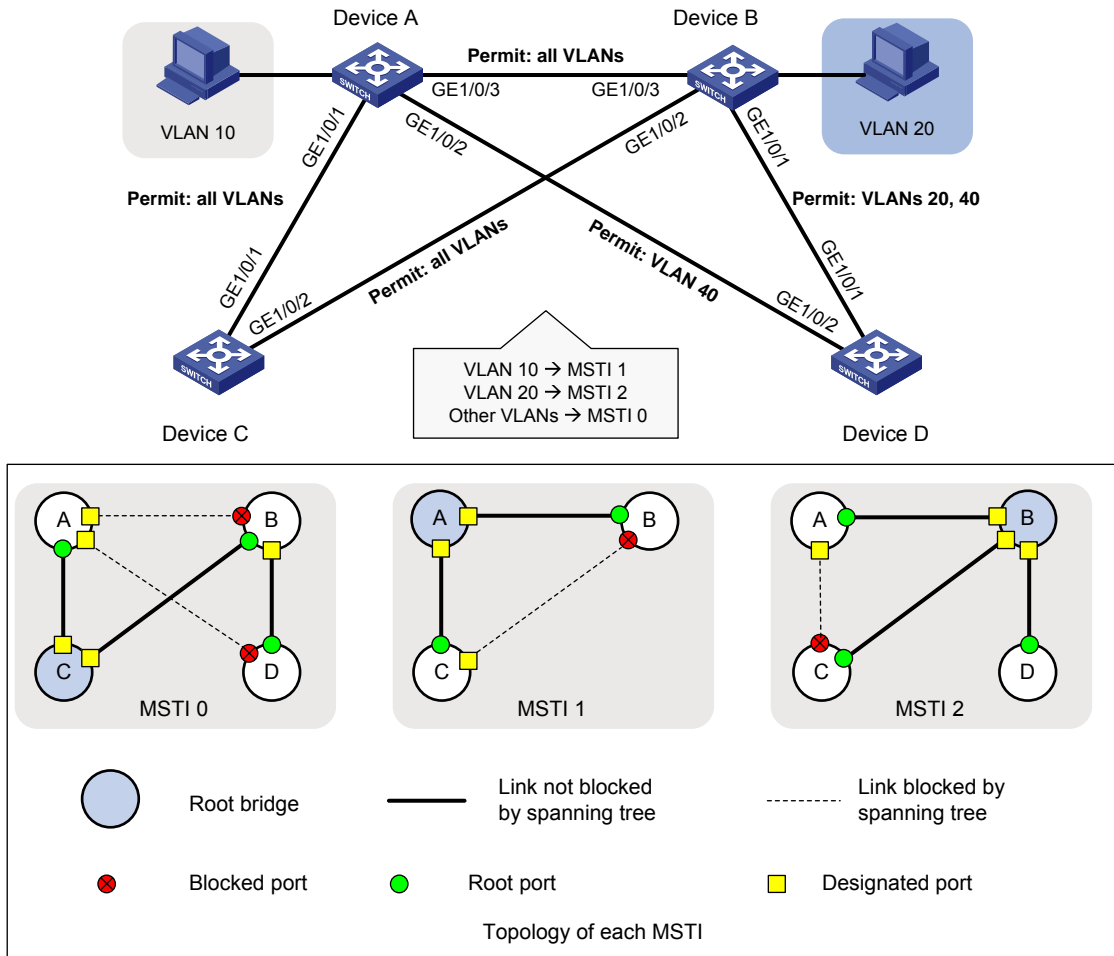
- Create VLAN 10 on Device A and VLAN 20 on Device B.
- Configure MSTP, map VLAN 10 to MSTI 1, map VLAN 20 to MSTI 2, and map the other VLANs to MSTI 0.

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.

When the network is stable, set the MVRP registration mode to **fixed** on the port of Device B connected to Device A. Then, dynamic VLANs on the port will not be deregistered.

Figure 57 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

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:

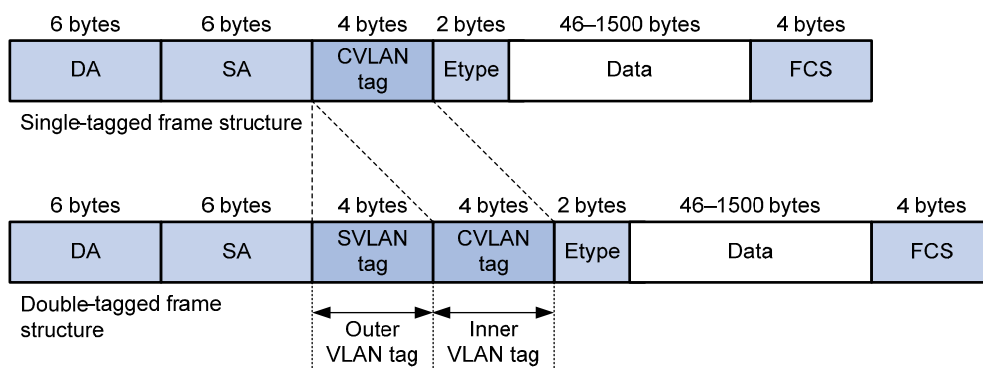
- Enables a service provider to use a single SVLAN to convey multiple CVLANs for a customer.
- Enables customers to plan CVLANs without conflicting with SVLANs.
- Enables customers to keep their VLAN assignment schemes unchanged when the service provider changes its VLAN assignment scheme.
- Allows customers 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 58](#), a QinQ frame transmitted over the service provider network carries the following tags:

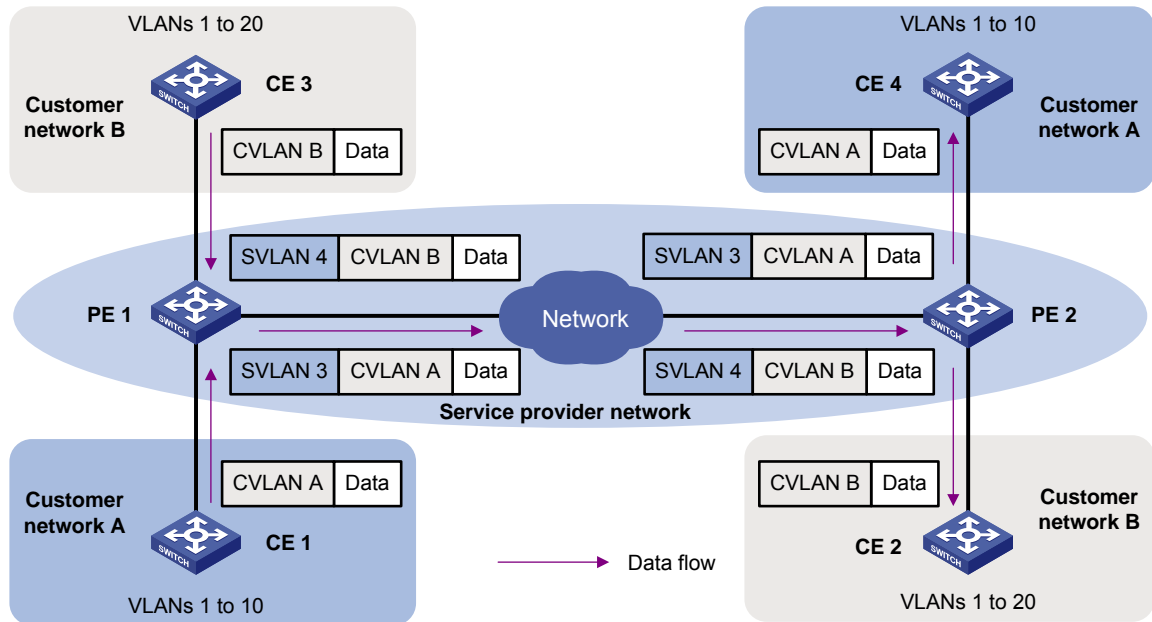
- **CVLAN tag**—Identifies the VLAN to which the frame belongs when it is transmitted in the customer network.
- **SVLAN tag**—Identifies the VLAN to which the QinQ frame belongs when it is transmitted in the service provider network. The service provider allocates the SVLAN tag to the customer.

Figure 58 Single-tagged Ethernet frame header and double-tagged Ethernet frame header



The devices in the service provider network forward a tagged frame according to its SVLAN tag only. The CVLAN tag is transmitted as part of the frame's payload.

Figure 59 Typical QinQ application scenario



As shown in [Figure 59](#), customer network A has CVLANs 1 through 10. Customer network B has CVLANs 1 through 20. The service provider assigns SVLANs 3 and 4 to customer networks A and B, respectively.

1. When a tagged Ethernet frame from customer network A arrives at PE 1, the PE tags the frame with SVLAN 3. When a tagged Ethernet frame from customer network B arrives at PE 1, the PE tags the frame with SVLAN 4.
2. The double-tagged Ethernet frame is then transmitted over the service provider network and arrives at the other PE. The PE removes the SVLAN tag of the frame before sending it to the target CE.

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:

- If QinQ conflicts with one-to-two VLAN mapping, 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. 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 <i>interface-type</i> <i>interface-number</i>	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 <i>interface-type</i> <i>interface-number</i>	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.	<ul style="list-style-type: none"> • For hybrid ports: port hybrid vlan <i>vlan-id-list</i> { tagged untagged } • For trunk ports: 	By default, trunk ports allow only packets from VLAN 1 to pass through. Hybrid ports allow only packets from

Step	Command	Remarks
	port trunk permit vlan { <i>vlan-id-list</i> all }	VLAN 1 to pass through untagged.
5. Enable QinQ on the port.	qinq enable	By default, QinQ is disabled.
6. Specify transparent VLANs.	qinq transparent-vlan <i>vlan-list</i>	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 configure 0x8200 and 0x9100 as the CVLAN TPID and SVLAN TPID 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 15](#).

Table 15 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

Protocol type	Value
Cluster	0x88A7
Reserved	0xFFFFD/0xFFFFE/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 <i>hex-value</i>	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 <i>interface-type interface-number</i>	N/A
3. Configure the SVLAN TPID.	qinq ethernet-type service-tag <i>hex-value</i>	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	traffic classifier <i>classifier-name</i> [operator	By default, no traffic

Step	Command	Remarks
enter traffic class view.	{ and or }	class is configured.
3. Configure CVLAN match criteria.	<ul style="list-style-type: none"> Match CVLAN IDs: if-match customer-vlan-id <i>vlan-id-list</i> Match 802.1p priority: if-match customer-dot1p <i>dot1p-value</i><1-8> 	N/A
4. Return to system view.	quit	N/A
5. Create a traffic behavior and enter traffic behavior view.	traffic behavior <i>behavior-name</i>	N/A
6. Configure a priority marking action for SVLAN tags.	<ul style="list-style-type: none"> Replace the priority in the SVLAN tags of matching frames with the configured priority: remark dot1p <i>dot1p-value</i> 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 <i>policy-name</i>	N/A
9. Associate the traffic class with the traffic behavior.	classifier <i>classifier-name</i> behavior <i>behavior-name</i>	N/A
10. Return to system view.	quit	N/A
11. Enter Layer 2 Ethernet interface view.	interface <i>interface-type interface-number</i>	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 <i>policy-name inbound</i>	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 <i>interface-type</i> <i>interface-number</i>]

QinQ configuration examples

Basic QinQ configuration example

Network requirements

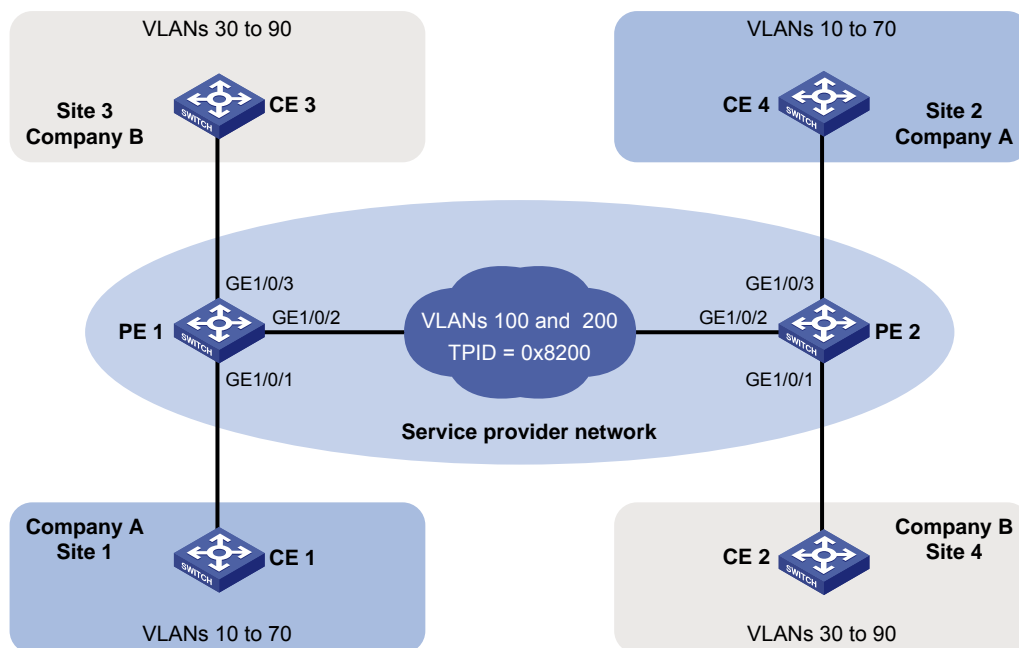
As shown in [Figure 60](#):

- 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 of Customer A and Company B in VLANs 100 and 200, 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 60 Network diagram



Configuration procedure

1. Configuring 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. Configuring 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. Configuring 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

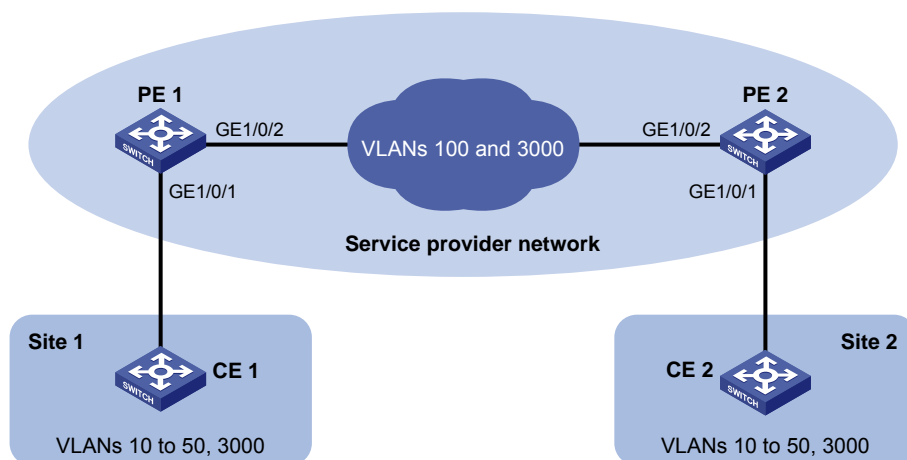
As shown in [Figure 61](#):

- 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 61 Network diagram



Configuration procedure

1. Configuring PE 1:

Configure system 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. Configuring 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. Configuring 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

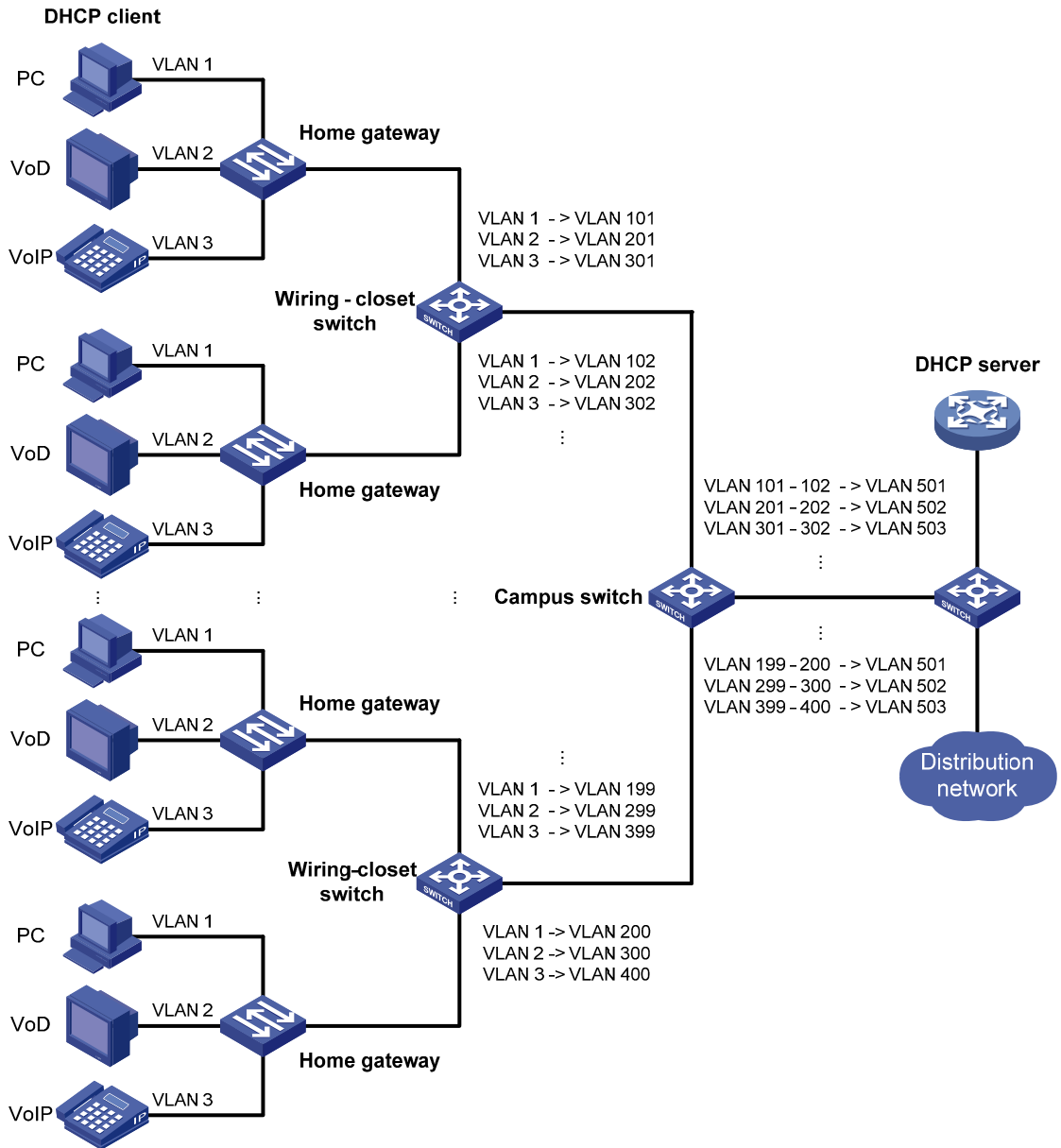
VLAN mapping re-marks VLAN tagged traffic with new VLAN IDs. Hewlett Packard Enterprise provides the following types of VLAN mapping:

- **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 62](#) 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 62 Application scenario of one-to-one and many-to-one VLAN mapping



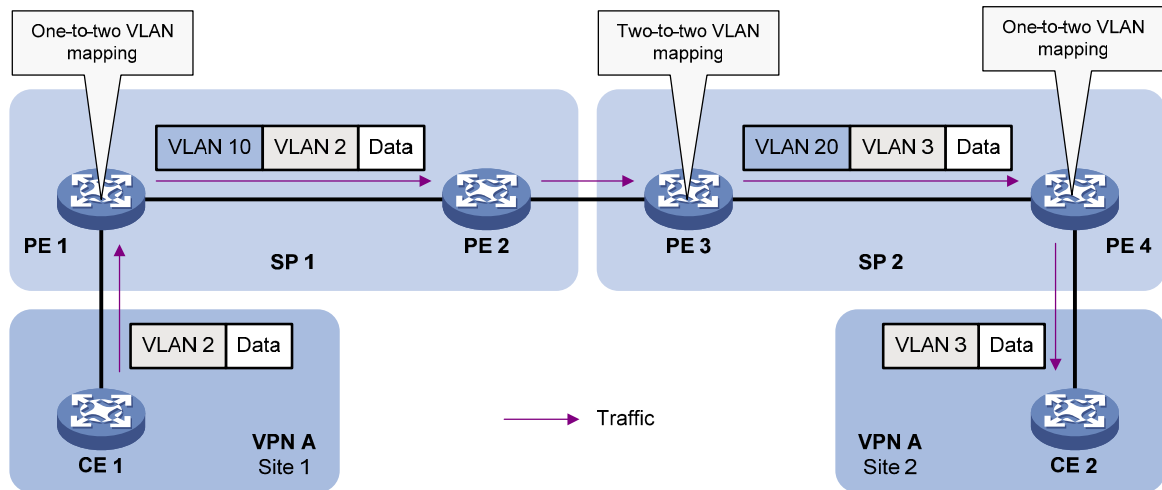
As shown in Figure 62, the network is implemented as follows:

- 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 63 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 63 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.

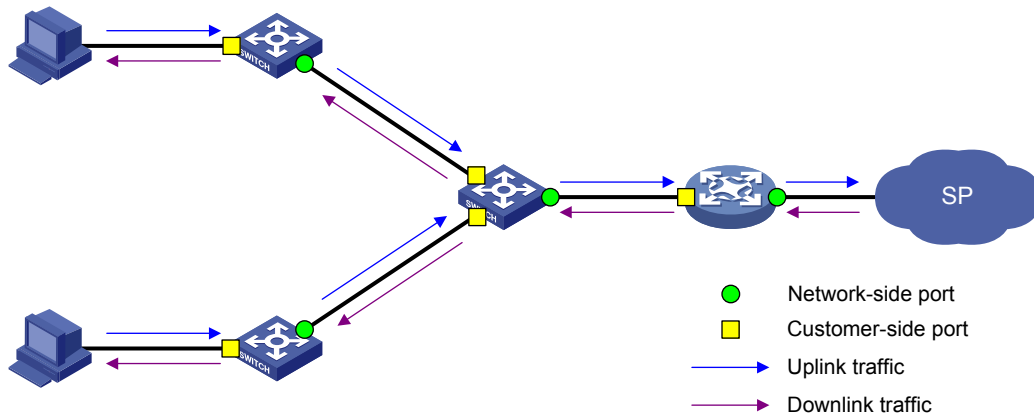
VLAN mapping implementations

Figure 64 shows a simplified network to help explain the concepts and terms in VLAN mapping.

These basic concepts 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 64 Basic VLAN mapping concepts

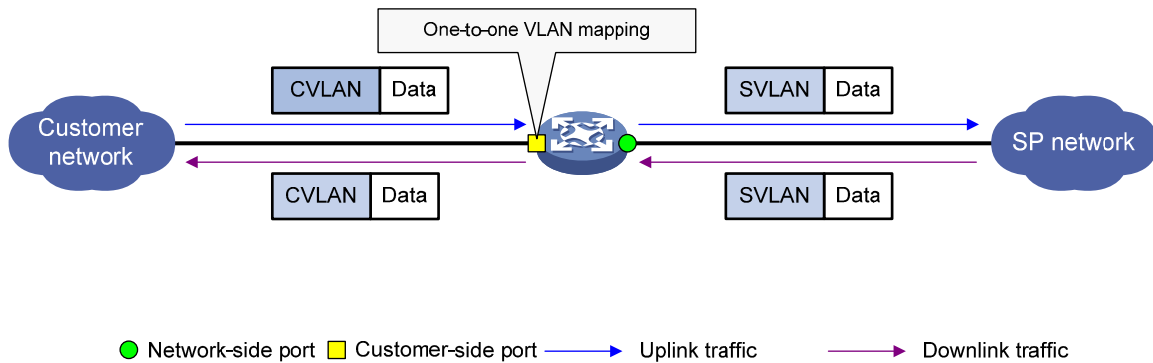


One-to-one VLAN mapping

As shown in Figure 65, 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 65 One-to-one VLAN mapping implementation

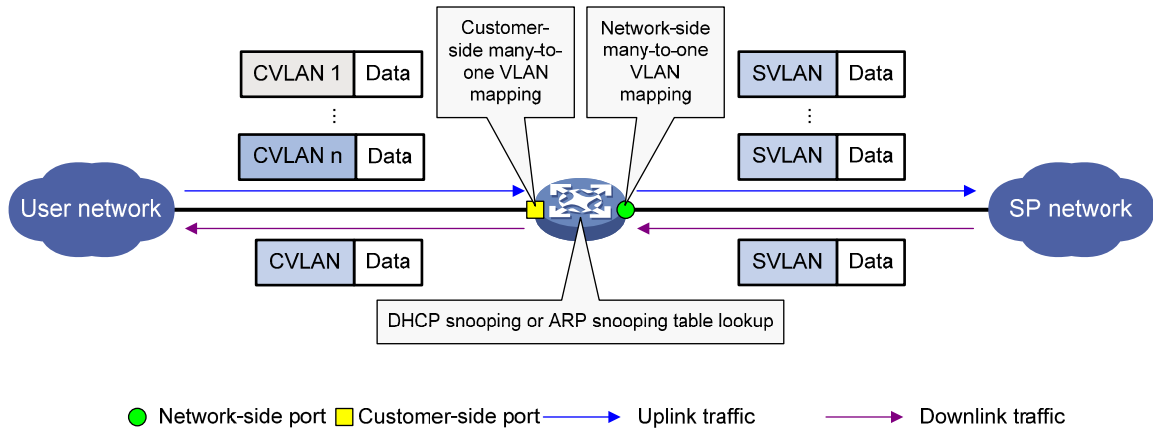


Many-to-one VLAN mapping

As shown in Figure 66, 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 66 Many-to-one VLAN mapping implementation



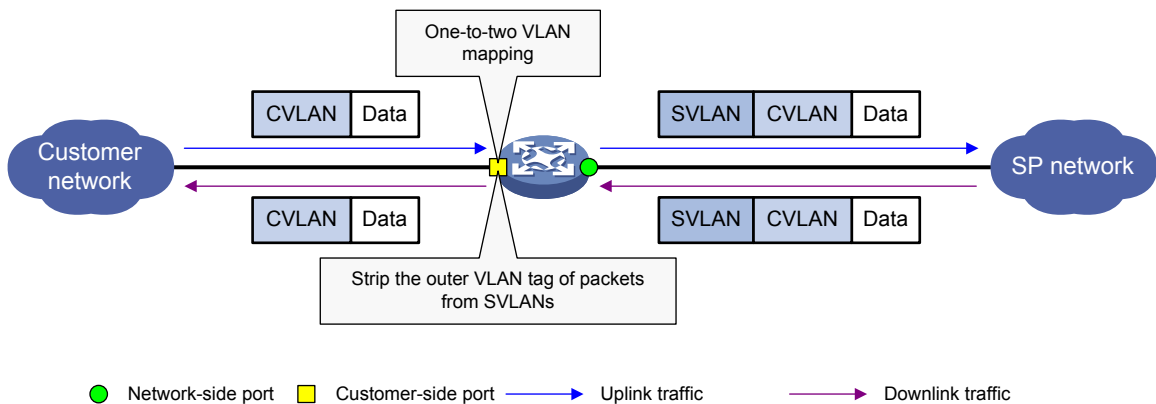
One-to-two VLAN mapping

As shown in Figure 67, 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 for 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 67 One-to-two VLAN mapping implementation

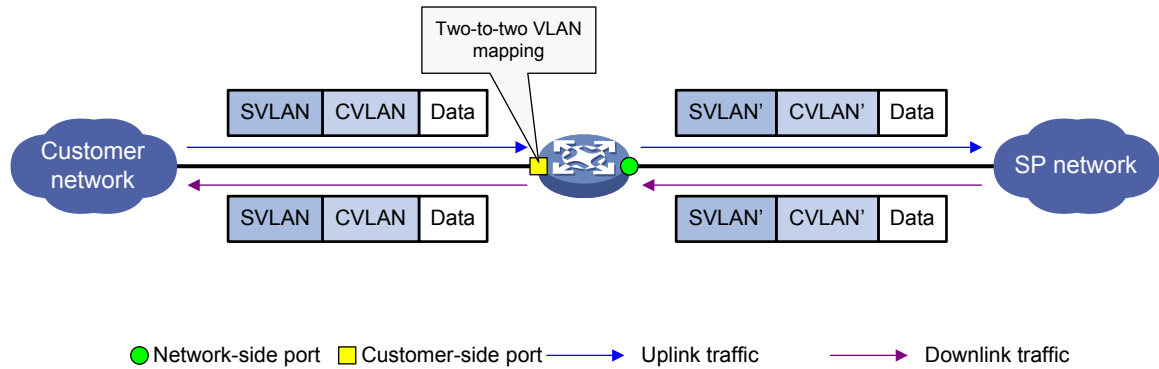


Two-to-two VLAN mapping

As shown in Figure 68, 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 68 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. However, 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 shown in Figure 62 .
Configuring many-to-one VLAN mapping <ul style="list-style-type: none"> • 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 shown in Figure 62 . 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 shown in Figure 63 , 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 shown in Figure 63 , 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 62](#)) 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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	N/A
3. Set the link type of the port.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> port trunk permit vlan <i>vlan-id-list</i> port hybrid vlan <i>vlan-id-list</i> tagged 	N/A
5. Configuring one-to-one VLAN mapping.	vlan mapping <i>vlan-id</i> translated-vlan <i>vlan-id</i>	By default, VLAN mapping is not configured on an interface.

Configuring many-to-one VLAN mapping

Configure many-to-one VLAN mapping on campus switches (see [Figure 62](#)) 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 VLAN.
- Customer-side many-to-one VLAN mapping is not supported on Layer 2 aggregate interfaces.
- To modify many-to-one VLAN mapping, 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 <i>Layer 3—IP Services Command Reference</i> .

Enabling ARP detection

Enable ARP detection for all involved VLANs, including 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 <i>vlan-id</i>	N/A
3. Enable ARP detection.	arp detection enable	By default, ARP detection is disabled. For more information about ARP detection configuration commands, see <i>Security Command Reference</i> .

Configuring the customer-side port

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the link type of the port.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> port trunk permit vlan <i>vlan-id-list</i> port hybrid vlan <i>vlan-id-list</i> tagged 	N/A
5. Configure many-to-one VLAN mapping.	vlan mapping uni { range <i>vlan-range-list</i> single <i>vlan-id-list</i> } translated-vlan <i>vlan-id</i>	By default, VLAN mapping is not 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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	N/A
3. Set the link type of the port.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> port trunk permit vlan <i>vlan-id-list</i> port hybrid vlan <i>vlan-id-list</i> tagged 	N/A
5. Configuring 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 trusted port.	arp detection trust	By default, all ports are ARP untrusted ports.
7. Configure many-to-one VLAN mapping.	vlan mapping nni	By default, VLAN mapping is not configured on an interface.

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 VLAN.
- 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** command to clear this ARP snooping entry by specifying the **ip ip-address** option.
 - 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 mapping, use the **reset arp snooping vlan vlan-id** command to clear the ARP snooping entries in each CVLAN.

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 all involved VLANs, including the original VLANs and the translated VLANs.

To enable ARP snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
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 <i>Layer 3—IP Services Command Reference</i> .

Configuring the customer-side port

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

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the link type of the port.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> port trunk permit vlan <i>vlan-id-list</i> port hybrid vlan <i>vlan-id-list</i> tagged 	N/A
5. Configure many-to-one VLAN mapping.	vlan mapping uni { range <i>vlan-range-list</i> single <i>vlan-id-list</i> } translated-vlan <i>vlan-id</i>	By default, VLAN mapping is not 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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	N/A
3. Set the link type of the port.	<ul style="list-style-type: none"> 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 VLAN.	<ul style="list-style-type: none"> port trunk permit vlan <i>vlan-id-list</i> port hybrid vlan <i>vlan-id-list</i> tagged 	N/A
5. Configure many-to-one VLAN mapping.	vlan mapping nni	By default, VLAN mapping is not configured on an interface.

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 63](#). One-to-two VLAN mapping enables the edge devices to add an outer VLAN tag to each incoming packet.

Before you configure one-to-two VLAN mapping, create the original VLAN and the translated VLAN.

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 four bytes. As a best practice, set the MTU to a minimum of 1504 bytes on interfaces in the service provider network when you configure one-to-two VLAN mapping.

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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	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 original VLANs.	port hybrid vlan <i>vlan-id-list</i> { 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 translated outer VLANs as an untagged member.	port hybrid vlan <i>vlan-id-list</i> 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 one-to-two VLAN mapping.	vlan mapping nest { range <i>vlan-range-list</i> single <i>vlan-id-list</i> } nested-vlan <i>vlan-id</i>	By default, VLAN mapping is not 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 63](#). 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.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> 	N/A
3. Set the link type of the port.	<ul style="list-style-type: none"> Configure the port as a trunk 	By default, the link type of a

Step	Command	Remarks
	port: port link-type trunk <ul style="list-style-type: none"> Configure the port as a hybrid port: port link-type hybrid 	port is access .
4. Assign the port to the original VLANs and the translated VLANs.	<ul style="list-style-type: none"> port trunk permit vlan <i>vlan-id-list</i> port hybrid vlan <i>vlan-id-list</i> tagged 	N/A
5. Configure two-to-two VLAN mapping.	vlan mapping tunnel <i>outer-vlan-id</i> <i>inner-vlan-id</i> translated-vlan <i>outer-vlan-id</i> <i>inner-vlan-id</i>	By default, VLAN mapping is not 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 <i>interface-type</i> <i>interface-number</i>]

VLAN mapping configuration examples

One-to-one and many-to-one VLAN mapping configuration example

Network requirements

As shown in [Figure 69](#):

- 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.

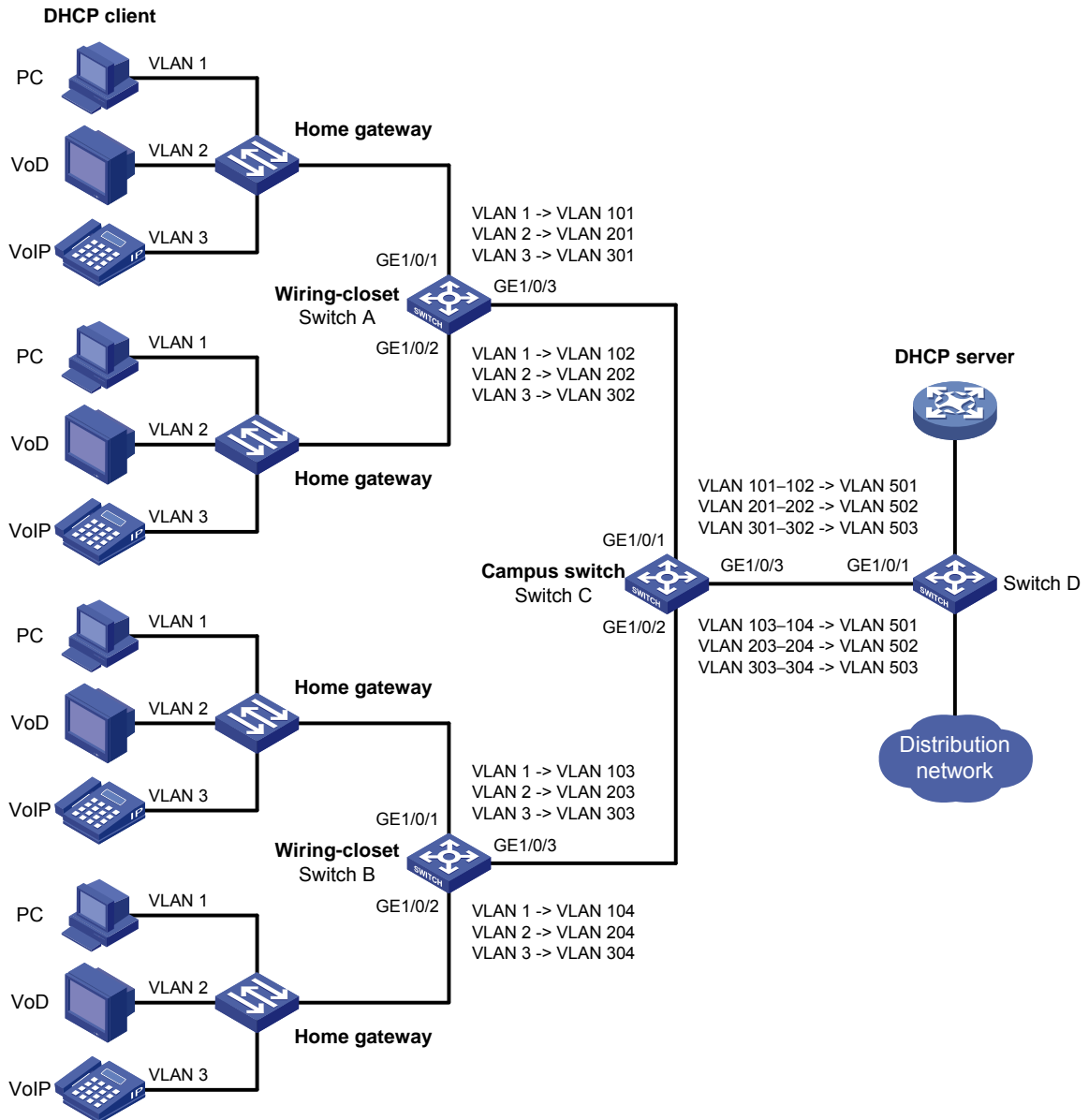
To isolate traffic of the same service type from different households, configure one-to-one VLAN mapping on the wiring-closet switches. This feature assigns one VLAN to each type of traffic from each household.

To save VLAN resources, configure many-to-one VLAN mapping 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 16 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 69 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 mapping 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 mapping 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 mapping 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 mapping 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 many-to-one VLAN mapping on the network-side port GigabitEthernet 1/0/3.

```
[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

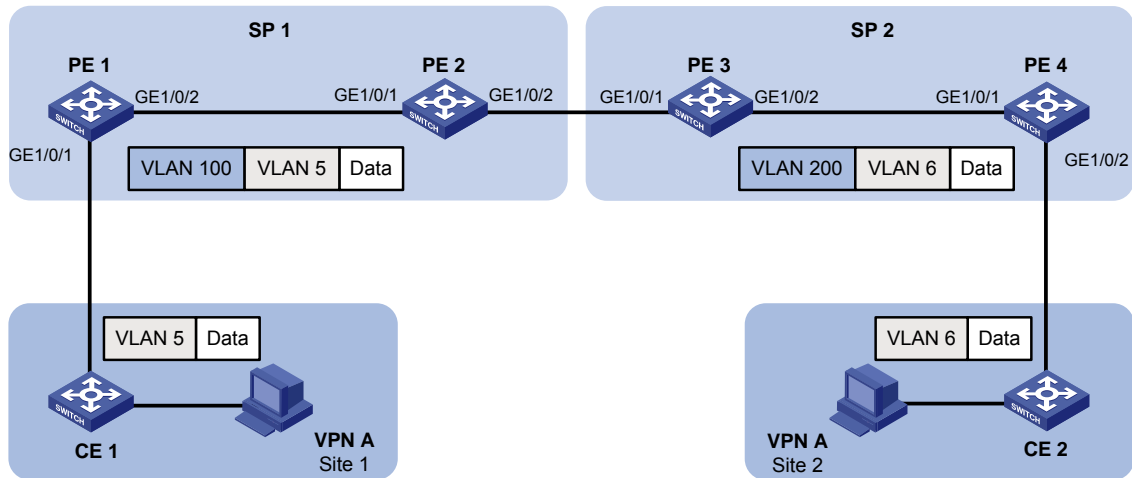
As shown in [Figure 70](#):

- 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 mapping and two-to-two VLAN mapping to enable the two branches to communicate across networks SP 1 and SP 2.

Figure 70 Network diagram



Configuration procedure

1. Configure PE 1:

Configure 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 two-to-two VLAN mapping on GigabitEthernet 1/0/1 to map SVLAN 100 and CVLAN 5 to SVLAN 200 and CVLAN 6, respectively.

```
[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 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

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:

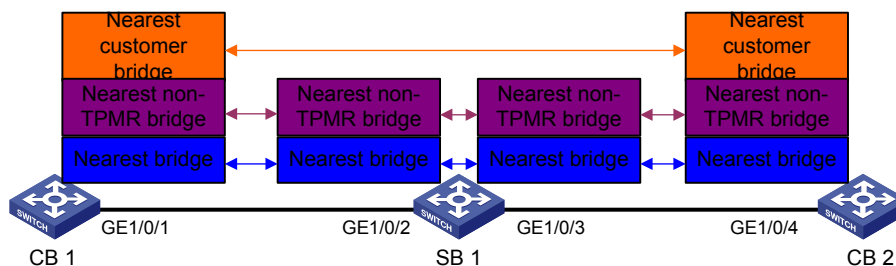
- Nearest bridge agent.
- Nearest customer bridge agent.
- Nearest non-TPMR bridge agent.

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 71](#) shows the neighbor relationships for these LLDP agents. LLDP has two bridge modes: customer bridge (CB) and service bridge (SB).

Figure 71 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 72 Ethernet II-encapsulated LLDP frame

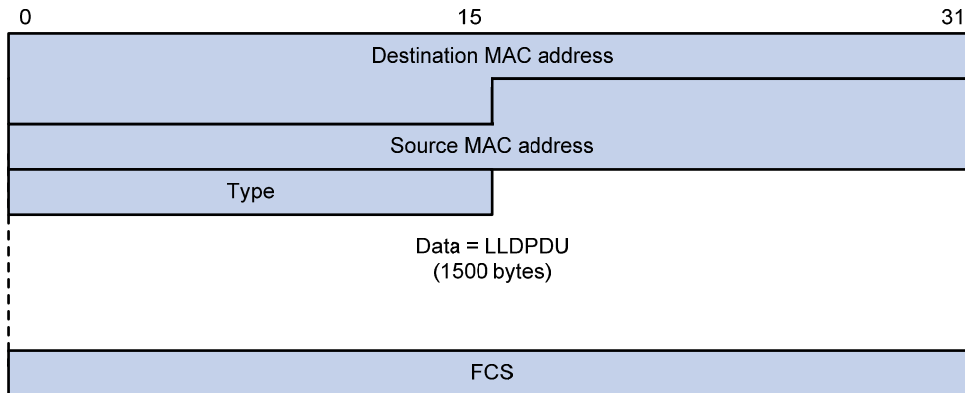


Table 17 Fields in an Ethernet II-encapsulated LLDP frame

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: <ul style="list-style-type: none"> • 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 73 SNAP-encapsulated LLDP frame

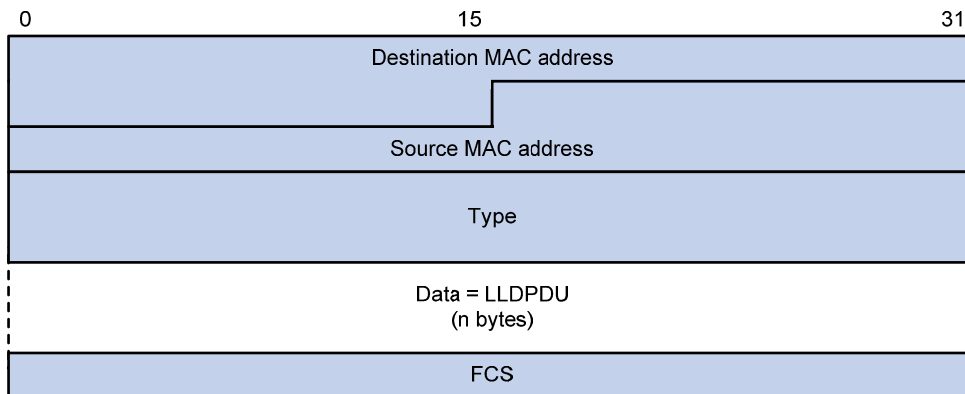


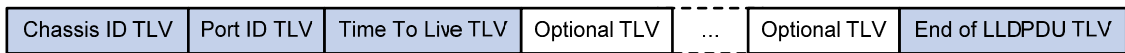
Table 18 Fields in a SNAP-encapsulated LLDP frame

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 74](#).

Figure 74 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 19](#) lists the basic management TLV types. Some of them are mandatory for LLDPDUs.

Table 19 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: <ul style="list-style-type: none"> • 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.	

Type	Description	Remarks
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: <ul style="list-style-type: none"> 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 20 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.

- IEEE 802.3 organizationally specific TLVs

Table 21 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: <ul style="list-style-type: none"> Port class (PSE or PD).

Type	Description
	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 22](#).

Table 22 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.
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

Type	Description
	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: <ul style="list-style-type: none">• (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.) Disabling PVID inconsistency check
(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. 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: <ul style="list-style-type: none">• If the switch starts up with empty configuration, LLDP is disabled globally (initial setting).

Step	Command	Remarks
		<ul style="list-style-type: none"> If the switch starts up with the default configuration file, LLDP is enabled globally (factory default). <p>For more information about empty configuration and the default configuration file, see <i>Fundamentals Configuration Guide</i>.</p>
3. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or IRF physical interface view.	interface <i>interface-type interface-number</i>	You can configure LLDP on an IRF physical interface to check its connections and link status. IRF physical interfaces support only nearest bridge agents.
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:

- 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 the VLAN.
- 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 the VLAN.

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 Ethernet interface view, Layer 2 aggregate interface view, or IRF physical interface view.	interface <i>interface-type interface-number</i>	N/A
3. Set the LLDP operating	<ul style="list-style-type: none"> In Layer 2 Ethernet interface view: lldp [agent { nearest-customer 	By default:

Step	Command	Remarks
mode.	<p>nearest-nontpmr }] admin-status { disable rx tx txrx }</p> <ul style="list-style-type: none"> In Layer 2 aggregate interface view: lldp agent { nearest-customer nearest-nontpmr } admin-status { disable rx tx txrx } In IRF physical interface view: lldp admin-status { disable rx tx txrx } 	<ul style="list-style-type: none"> The nearest bridge agent operates in txrx mode. The nearest customer bridge agent and nearest non-TPMR bridge agent operate in disable mode. <p>In Ethernet interface view, if no agent type is specified, the command configures the operating mode for nearest bridge agents.</p> <p>In aggregate interface view, you can configure the operating mode for only nearest customer bridge agents and nearest non-TPMR bridge agents.</p> <p>In IRF physical interface view, you can configure the operating mode for only nearest bridge agents.</p>

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 Ethernet interface view, Layer 2 aggregate interface view, or IRF physical interface view.	interface interface-type interface-number	N/A

Step	Command	Remarks
3. Enable LLDP polling and set the polling interval.	<ul style="list-style-type: none"> In Layer 2 Ethernet interface view: lldp [agent { nearest-customer nearest-nontpmr }] check-change-interval <i>interval</i> In Layer 2 aggregate interface view: lldp agent { nearest-customer nearest-nontpmr } check-change-interval <i>interval</i> In IRF physical interface view: lldp check-change-interval <i>interval</i> 	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 Ethernet interface view, Layer 2 aggregate interface view, or IRF physical interface view.	interface <i>interface-type interface-number</i>	N/A
3. Configure the advertisable TLVs (in Layer 2 Ethernet interface view).	<ul style="list-style-type: none"> lldp tlv-enable { basic-tlv { all port-description system-capability system-description system-name management-address-tlv [ipv6] [<i>ip-address</i>] } dot1-tlv { all port-vlan-id link-aggregation protocol-vlan-id [<i>vlan-id</i>] vlan-name [<i>vlan-id</i>] management-vid [<i>mvlan-id</i>] } dot3-tlv { all mac-physic max-frame-size power } med-tlv { all capability inventory network-policy [<i>vlan-id</i>] power-over-ethernet location-id { civic-address <i>device-type country-code</i> { <i>ca-type ca-value</i> }&<1-10> elin-address <i>tel-number</i> } } } lldp agent nearest-nontpmr tlv-enable { basic-tlv { all port-description system-capability system-description system-name management-address-tlv [ipv6] [<i>ip-address</i>] } dot1-tlv { all port-vlan-id link-aggregation } } lldp agent nearest-customer tlv-enable { basic-tlv { all port-description system-capability system-description system-name management-address-tlv [ipv6] [<i>ip-address</i>] } dot1-tlv { all port-vlan-id link-aggregation } } 	<p>By default:</p> <ul style="list-style-type: none"> Nearest bridge agents can advertise all types of LLDP TLVs except the 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.
4. Configure the advertisable TLVs (in Layer 2 aggregate interface view).	<ul style="list-style-type: none"> lldp agent nearest-nontpmr tlv-enable { basic-tlv { all management-address-tlv [ipv6] [<i>ip-address</i>] port-description system-capability system-description system-name } 	<p>By default:</p> <ul style="list-style-type: none"> Nearest non-TPMR bridge agents advertise no TLVs. Nearest customer

Step	Command	Remarks
	<pre> dot1-tlv { all port-vlan-id } • lldp agent nearest-customer tlv-enable { basic-tlv { all management-address-tlv [ipv6] [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] }</pre>	<p>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).</p> <p>Nearest bridge agents are not supported on Layer 2 aggregate interfaces.</p>
5. Configure the advertisable TLVs (in IRF physical interface view).	<pre>lldp tlv-enable basic-tlv { port-description system-capability system-description system-name }</pre>	By default, the LLDP agent can advertise all types of LLDP TLVs.

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 Ethernet interface view or Layer 2 aggregate interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Allow LLDP to advertise the management address in LLDP frames and configure the advertised management address.	<ul style="list-style-type: none"> • In Layer 2 Ethernet interface view: lldp [agent { nearest-customer nearest-nontpmr }] tlv-enable basic-tlv management-address-tlv [ipv6] [ip-address] • In Layer 2 aggregate interface view: lldp agent 	<p>By default:</p> <ul style="list-style-type: none"> • 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.

Step	Command	Remarks
	<pre>{ nearest-customer nearest-nontpmr } tlv-enable basic-tlv management-address-tlv [ipv6] [ip-address]</pre>	
4. Configure the encoding format of the management address as string.	<ul style="list-style-type: none"> In Layer 2 Ethernet interface view: <pre>lldp [agent { nearest-customer nearest-nontpmr }] management-address-for mat string</pre> In Layer 2 aggregate interface view: <pre>lldp agent { nearest-customer nearest-nontpmr } management-address-for mat string</pre> 	By default, the encoding format of the management address is numeric.

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:

$$\text{TTL} = \text{Min} (65535, (\text{TTL multiplier} \times \text{LLDP frame transmission interval} + 1))$$

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 <i>value</i>	The default setting is 4.
3. Set the LLDP frame transmission interval.	lldp timer tx-interval <i>interval</i>	The default setting is 30 seconds.
4. Set the token bucket size for sending LLDP frames.	lldp max-credit <i>credit-value</i>	The default setting is 5.
5. Set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.	lldp fast-count <i>count</i>	The default setting is 4.
6. Set the interval for fast LLDP frame transmission.	lldp timer fast-interval <i>interval</i>	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 should 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 Ethernet interface view, Layer 2 aggregate interface view, or IRF physical interface view.	interface <i>interface-type interface-number</i>	N/A
3. Set the encapsulation format for LLDP frames to SNAP.	<ul style="list-style-type: none"> • In Layer 2 Ethernet interface view: lldp [agent { nearest-customer nearest-nontpmr }] encapsulation snap • In Layer 2 aggregate interface view: lldp agent { nearest-customer nearest-nontpmr } encapsulation snap • In IRF physical interface view: lldp encapsulation snap 	By default, Ethernet II encapsulation format applies.

Disabling PVID inconsistency check

By default, the device requires that the PVID for both ends of a link must be identical. If the PVID in a received packet is different from the local PVID, the device generates logs to inform you of PVID inconsistency.

You can disable PVID inconsistency check if different PVIDs are required on a link. For example, access switches and distribution switches use different PVIDs on their in-between links to assign traffic to different VLANs.

To disable PVID inconsistency check:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable PVID inconsistency check.	lldp ignore-pvid-inconsistency	By default, PVID inconsistency check is enabled.

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.
- **Rx**—CDP packets can be received but cannot be transmitted.
- **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 Rx or 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 Ethernet interface view.	interface <i>interface-type interface-number</i>	N/A
4. Configure CDP-compatible LLDP to operate in Rx or TxRx mode.	lldp compliance admin-status cdp { rx 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 Ethernet interface view, Layer 2 aggregate interface view, or IRF physical interface view.	interface <i>interface-type interface-number</i>	N/A
3. Enable LLDP trapping.	<ul style="list-style-type: none"> In Layer 2 Ethernet interface view: lldp [agent { nearest-customer nearest-nontpmr }] notification remote-change enable In Layer 2 aggregate interface view: lldp agent { nearest-customer nearest-nontpmr } notification remote-change enable In IRF physical interface view: lldp notification remote-change enable 	By default, LLDP trapping is disabled.
4. Enable LLDP-MED trapping (in Layer 2 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 <i>interval</i>	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 <i>interface-type interface-number</i>]
Display the information contained in the LLDP TLVs sent from neighboring devices.	display lldp neighbor-information [[interface <i>interface-type interface-number</i>] [agent { nearest-bridge nearest-customer nearest-nontpmr }] [verbose]] list [system-name system-name]]
Display LLDP statistics.	display lldp statistics [global [interface <i>interface-type interface-number</i>] [agent { nearest-bridge nearest-customer nearest-nontpmr }]]
Display LLDP status of a port.	display lldp status [interface <i>interface-type interface-number</i>] [agent { nearest-bridge nearest-customer nearest-nontpmr }]
Display types of advertisable optional LLDP TLVs.	display lldp tlv-config [interface <i>interface-type interface-number</i>] [agent { nearest-bridge nearest-customer nearest-nontpmr }]

LLDP configuration examples

Basic LLDP configuration example

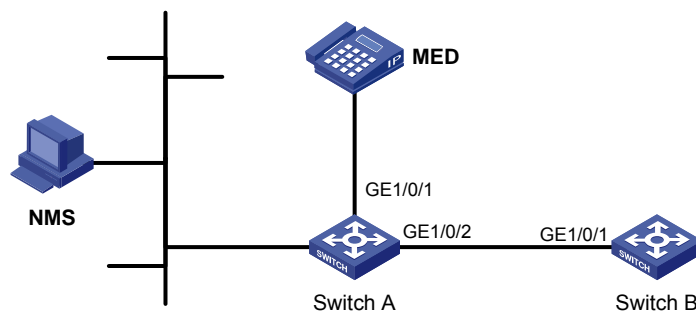
Network requirements

As shown in [Figure 75](#), the NMS and Switch A are located in the same Ethernet network. A MED device and Switch B are connected to GigabitEthernet1/0/1 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 75 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-nontpnr:

```
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-nontpnr:
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

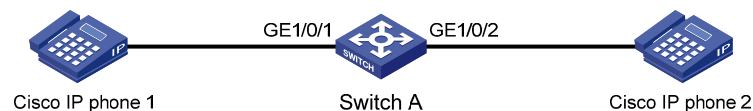
Network requirements

As shown in [Figure 76](#), 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 76 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

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.
<i>Italic</i>	<i>Italic</i> 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 appears; 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 card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

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 mappingapplication scenario, 208
- 1 VLAN mappingconfiguration, 214, 220
- 1 VLAN mappingimplementation, 210, 211
- 2 VLAN mappingapplication scenario, 210
- 2 VLAN mappingconfiguration, 218, 224
- 2 VLAN mappingimplementation, 210, 212

2\

- 2 VLAN mappingapplication scenario, 210
- 2 VLAN mappingconfiguration, 219, 224
- 2 VLAN mappingimplementation, 210, 212

802

- 802.1Q-in-802.1Q. Use QinQ
- QinQ SVLAN tag 802.1p priority, 202
- VLAN group configuration, 136

802.x

- 802.1 LLDPDU TLV types, 230
- 802.3 LLDPDU TLV types, 230

A

accessing

- port-based VLAN assignment (access port), 127

action

- loop detection block, 117
- loop detection no-learning protection, 117
- loop detection shutdown protection, 117

adding

- MAC address table blackhole entry, 20
- MAC address table multiport unicast entry, 20

address

- MAC address learning disable, 21
- MAC address move notification, 25
- MAC address table address synchronization, 24
- MAC Information queue length, 31
- SNMP notification for MAC address table, 28
- static source check disable, 27

advertising

- authorization VLANs through LLDP/CDP dynamically, 177
- LAN switching LLDP advertisable TLV, 237

aggregating

- link. See [link aggregation](#)

aging

- LAN switching spanning tree max age timer, 79
- MAC address table timer, 22

algorithm

- LAN switching STP calculation, 60

alternate port (MST), 69

ARP

- ARP fast update enabling for MAC address move, 26

ARP detection

- VLAN M\1 mapping (dynamic IP address assignment), 215

ARP snooping

- VLAN M\1 mapping (static IP address assignment), 217

assigning

- Layer 2 LAN switching port to isolation group (multiple), 55
- port-based VLAN access port (interface view), 127
- port-based VLAN access port (VLAN view), 127
- port-based VLAN hybrid port, 128
- port-based VLAN trunk port, 128
- voice VLAN assignment mode, 170

attribute

- Ethernet link aggregation attribute configuration, 35

auto

- interface auto power-down (Ethernet), 5
- loop detection port status auto recovery, 117

automatic

- voice VLAN assignment mode, 170
- voice VLAN automatic assignment mode port operation configuration, 174, 178

AutoMDIX mode (Ethernet interface), 10

B

backing up

- LAN switching MST backup port, 69

bandwidth

- Ethernet link aggregate interface (expected bandwidth), 44

basic management LLDPDU TLV types, 230

BFD

- Ethernet link aggregation group BFD, 44

blackhole entry

- MAC address table, 17, 20

block action (loop detection), 117

boundary port (MST), 69

BPDU

- LAN switching MST region max hops, [78](#)
- LAN switching spanning tree BPDU drop, [98](#)
- LAN switching spanning tree BPDU guard, [95](#)
- LAN switching spanning tree hello time, [79](#)
- LAN switching spanning tree max age timer, [79](#)
- LAN switching spanning tree TC-BPDU guard, [97](#)
- LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
- LAN switching STP BPDU forwarding, [64](#)
- LAN switching transmission rate configuration, [80](#)

bridge

- LAN switching LLDP agent customer bridge, [228](#)
- LAN switching LLDP agent nearest bridge, [228](#)
- LAN switching LLDP agent non-TPMR bridge, [228](#)

bridging

- LAN switching MST common root bridge, [68](#)
- LAN switching MST regional root, [68](#)
- LAN switching spanning tree loop guard, [96](#)
- LAN switching spanning tree root bridge, [76](#)
- LAN switching spanning tree root bridge (device), [77](#)
- LAN switching spanning tree root guard, [95](#)
- LAN switching spanning tree secondary root bridge (device), [77](#)
- LAN switching STP designated bridge, [59](#)
- LAN switching STP root bridge, [59](#)

bulk

- interface configuration, [15](#)
- interface configuration display, [16](#)
- interface configuration restrictions, [15](#)

C

cable

- interface cable connection (Layer 2 Ethernet), [10](#)

calculating

- LAN switching MSTI calculation, [70](#)
- LAN switching MSTP CIST calculation, [70](#)
- LAN switching spanning tree port path cost calculation standard, [82](#)
- LAN switching spanning tree timeout factor, [80](#)
- LAN switching STP algorithm, [60](#)

CDP

- advertising authorization VLANs through LLDP dynamically, [177](#)

advertising voice VLAN information to IP phones, [169](#)

configuring LLDP/CDP to advertise a voice VLAN, [176](#)

LAN switching LLDP CDP compatibility, [240](#)

LAN switching LLDP CDP-compatible configuration, [247](#)

CE

L2PT configuration, [107](#), [109](#), [111](#)

L2PT for LACP configuration, [112](#)

L2PT for STP configuration, [111](#)

checking

LAN switching spanning tree No Agreement Check, [91](#), [93](#)

choosing

Ethernet link aggregation reference port, [36](#), [38](#)

Cisco

LAN switching LLDP CDP compatibility, [240](#)

LAN switching LLDP configuration (CDP-compatible), [247](#)

CIST

calculation, [70](#)

network device connection, [68](#)

spanning tree max age timer, [79](#)

combo interface, [1](#)

common root bridge, [68](#)

configuring

basic QinQ, [204](#)

Ethernet aggregate interface, [42](#)

Ethernet aggregate interface (description), [42](#)

Ethernet link aggregation, [34](#), [40](#), [48](#)

Ethernet link aggregation (Layer 2 dynamic), [50](#)

Ethernet link aggregation (Layer 2 static), [48](#)

Ethernet link aggregation group, [41](#)

Ethernet link aggregation group (dynamic), [42](#)

Ethernet link aggregation group (Layer 2 dynamic), [42](#)

Ethernet link aggregation group (Layer 2 static), [41](#)

Ethernet link aggregation group (static), [41](#)

Ethernet link aggregation group BFD, [44](#)

Ethernet link aggregation group load sharing, [46](#)

Ethernet link aggregation load sharing (Layer 2), [52](#)

interface (Ethernet combo), [1](#)

interface (Ethernet), [1](#)

interface (inloopback), [14](#)

interface (loopback), [13](#)

interface (null), [13](#)

interface basic settings (Ethernet), [2](#)

interface common settings (Ethernet), [1](#)

interface generic flow control (Ethernet), [4](#)
 interface jumbo frame support (Ethernet), [2](#)
 interface physical state change suppression (Ethernet), [3](#)
 interface storm control (Layer 2 Ethernet), [7](#)
 interface storm suppression (Layer 2 Ethernet), [6](#)
 IP subnet-based VLAN, [134](#), [141](#)
 L2PT, [107](#), [109](#), [111](#)
 L2PT for LACP, [112](#)
 L2PT for STP, [111](#)
 LAN switching LLDP, [228](#), [234](#), [243](#)
 LAN switching LLDP (CDP-compatible), [247](#)
 LAN switching LLDP advertisable TLVs, [237](#)
 LAN switching LLDP basics, [234](#), [243](#)
 LAN switching LLDP bridge mode, [235](#)
 LAN switching LLDP CDP compatibility, [240](#)
 LAN switching LLDP management address, [238](#)
 LAN switching LLDP management address encoding format, [238](#)
 LAN switching LLDP trapping, [242](#)
 LAN switching LLDP-MED trapping, [242](#)
 LAN switching MST region, [75](#)
 LAN switching MST region max hops, [78](#)
 LAN switching MSTP, [74](#), [100](#)
 LAN switching PVST, [73](#), [103](#)
 LAN switching RSTP, [72](#)
 LAN switching spanning tree, [58](#), [71](#), [100](#)
 LAN switching spanning tree BPDU transmission rate, [80](#)
 LAN switching spanning tree device priority, [77](#)
 LAN switching spanning tree Digest Snooping, [89](#), [90](#)
 LAN switching spanning tree edge port, [81](#)
 LAN switching spanning tree No Agreement Check, [91](#), [93](#)
 LAN switching spanning tree port link type, [85](#)
 LAN switching spanning tree port mode, [86](#)
 LAN switching spanning tree port path cost, [81](#), [84](#)
 LAN switching spanning tree port priority, [85](#)
 LAN switching spanning tree port role restriction, [96](#)
 LAN switching spanning tree protection functions, [94](#)
 LAN switching spanning tree root bridge, [76](#)
 LAN switching spanning tree root bridge (device), [77](#)
 LAN switching spanning tree secondary root bridge, [76](#)
 LAN switching spanning tree secondary root bridge (device), [77](#)
 LAN switching spanning tree switched network diameter, [78](#)
 LAN switching spanning tree TC Snooping, [93](#)
 LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
 LAN switching spanning tree timeout factor, [80](#)
 LAN switching spanning tree timer, [79](#)
 LAN switching STP, [72](#)
 Layer 2 LAN switching port isolation, [55](#)
 Layer 2 LAN switching port isolation (multiple isolation groups), [56](#)
 LLDP/CDP to advertise a voice VLAN, [176](#)
 loop detection, [116](#), [118](#), [120](#)
 loop detection protection action, [119](#)
 loop detection protection action (global), [119](#)
 loop detection protection action (Layer 2 aggregate interface), [119](#)
 loop detection protection action (Layer 2 Ethernet interface), [119](#)
 MAC address table, [17](#), [18](#), [28](#)
 MAC address table dynamic aging timer, [22](#)
 MAC address table entry, [19](#)
 MAC address table learning limit on interface, [23](#)
 MAC address table unknown frame forwarding rule, [23](#)
 MAC change notification interval, [31](#)
 MAC Information, [30](#), [31](#)
 MAC Information mode, [30](#)
 MAC Information queue length, [31](#)
 MAC-based VLAN, [129](#), [139](#)
 MVRP, [185](#), [188](#)
 MVRP registration mode, [186](#)
 MVRP timer, [187](#)
 port-based VLAN, [126](#), [137](#)
 private VLAN, [151](#), [152](#), [154](#)
 private VLAN promiscuous port, [154](#)
 private VLAN trunk promiscuous port, [157](#), [160](#)
 private VLAN trunk secondary port, [160](#)
 protocol-based VLAN, [135](#), [142](#)
 QinQ, [198](#), [204](#)
 QinQ CVLAN tag TPID value, [202](#)
 QinQ SVLAN tag TPID value, [202](#)
 QinQ VLAN tag TPID value, [201](#)
 QinQ VLAN transparent transmission, [200](#), [206](#)
 secondary VLAN Layer 3 communication, [165](#)
 super VLAN, [146](#), [146](#), [148](#)
 super VLAN interface, [147](#)
 VLAN, [123](#), [137](#)
 VLAN basic settings, [124](#)

- VLAN group, [136](#)
- VLAN interface basics, [125](#)
- VLAN mapping, [208](#), [213](#), [220](#)
- VLAN mapping (1\1), [214](#), [220](#)
- VLAN mapping (1\2), [218](#), [224](#)
- VLAN mapping (2\2), [219](#), [224](#)
- VLAN mapping (M\1), [214](#), [220](#)
- VLAN mapping (M\1)(dynamic IP address assignment), [215](#)
- VLAN mapping (M\1)(static IP address assignment), [217](#)
- VLAN mapping M\1 customer-side port (dynamic IP address assignment), [216](#)
- VLAN mapping M\1 customer-side port (static IP address assignment), [217](#)
- VLAN mapping M\1 network-side port (dynamic IP address assignment), [216](#)
- VLAN mapping M\1 network-side port (static IP address assignment), [218](#)
- voice VLAN, [168](#), [178](#)
- voice VLAN automatic assignment mode port operation, [174](#), [178](#)
- voice VLAN interface QoS priority settings, [173](#)
- voice VLAN manual assignment mode port operation, [175](#), [180](#)
- voice VLAN on a port, [170](#)
- connecting
 - interface cable connection (Layer 2 Ethernet), [10](#)
- cost
 - LAN switching spanning tree port path cost calculation standard, [82](#)
 - LAN switching spanning tree port path cost configuration, [81](#), [84](#)
 - LAN switching STP path cost, [60](#)
- creating
 - super VLAN sub VLAN, [146](#)
- CST
 - MST region connection, [68](#)
- customer
 - LAN switching LLDP customer bridge mode, [235](#)
- CVLAN
 - basic QinQ configuration, [204](#)
 - QinQ configuration, [198](#), [204](#)
 - QinQ VLAN transparent transmission configuration, [206](#)
 - VLAN mapping configuration, [208](#), [213](#), [220](#)
 - VLAN mapping implementation, [210](#)
- D**
- default
 - Ethernet link aggregate interface default settings, [45](#)
- designated
 - LAN switching MST port, [69](#)
 - LAN switching STP bridge, [59](#)
 - LAN switching STP port, [59](#)
- detecting
 - Ethernet link aggregation group BFD, [44](#)
- device
 - interface configuration (Ethernet), [1](#)
 - LAN switching LLDP basic configuration, [234](#), [243](#)
 - LAN switching LLDP CDP compatibility, [240](#)
 - LAN switching LLDP configuration, [228](#), [234](#), [243](#)
 - LAN switching LLDP configuration (CDP-compatible), [247](#)
 - LAN switching LLDP parameters, [239](#)
 - LAN switching MSTP implementation, [71](#)
 - LAN switching spanning tree BPDU drop, [98](#)
 - LAN switching spanning tree BPDU guard, [95](#)
 - LAN switching spanning tree Digest Snooping, [89](#), [90](#)
 - LAN switching spanning tree loop guard, [96](#)
 - LAN switching spanning tree No Agreement Check, [91](#), [93](#)
 - LAN switching spanning tree port role restriction, [96](#)
 - LAN switching spanning tree priority, [77](#)
 - LAN switching spanning tree protection functions, [94](#)
 - LAN switching spanning tree root guard, [95](#)
 - LAN switching spanning tree TC Snooping, [93](#)
 - LAN switching spanning tree TC-BPDU guard, [97](#)
 - LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
 - loop protection actions, [117](#)
 - MVRP configuration, [182](#), [185](#), [188](#)
 - spanning tree SNMP notification (new-root election, topology change events), [98](#)
- DHCP snooping
 - VLAN M\1 mapping (dynamic IP address assignment), [215](#)
- Digest Snooping (spanning tree), [89](#), [90](#)
- directing
 - Ethernet link aggregation traffic redirection, [47](#)
- disabling
 - MAC address learning, [21](#)
 - PVID inconsistency check, [240](#)
 - static source check, [27](#)
- discarding
 - LAN switching MST discarding port state, [69](#)
- displaying

- bulk interface configuration, 16
 - Ethernet link aggregation, 48
 - interface, 14
 - interface (Ethernet), 12
 - L2PT, 110
 - LAN switching LLDP, 242
 - LAN switching spanning tree, 99
 - Layer 2 LAN switching port isolation, 55
 - loop detection, 120
 - MAC address table, 28
 - MVRP, 188
 - private VLAN, 154
 - QinQ, 203
 - subinterface (Ethernet), 12
 - super VLAN, 147
 - VLAN, 137
 - VLAN mapping, 220
 - voice VLAN, 177
 - dot1d-1998 (STP port path cost calculation), 82
 - dot1s (STP port mode), 86
 - dot1t (STP port path cost calculation), 82
 - dynamic
 - configuring MAC-based VLAN dynamic assignment, 133
 - Ethernet link aggregation (dynamic mode), 37
 - Ethernet link aggregation (Layer 2), 50
 - Ethernet link aggregation group, 42
 - Ethernet link aggregation group BFD, 44
 - Ethernet link aggregation mode, 35
 - Layer 2 Ethernet link aggregation group, 42
 - MAC address table dynamic aging timer, 22
 - MAC address table entry, 17
 - MAC-based VLAN dynamic assignment, 130
- ## E
- edge port
 - LAN switching MST, 69
 - spanning tree, 81
 - EEE energy saving, 5
 - enabling
 - ARP fast update for MAC address move, 26
 - bridging (Ethernet interface), 11
 - Ethernet link aggregation traffic redirection, 47
 - interface auto power-down (Ethernet), 5
 - interface EEE energy saving, 5
 - interface energy-saving functions (Ethernet), 5
 - L2PT, 109, 109
 - LAN switching LLDP, 234
 - LAN switching LLDP polling, 236
 - LAN switching spanning tree BPDU drop, 98
 - LAN switching spanning tree BPDU guard, 95
 - LAN switching spanning tree feature, 87
 - LAN switching spanning tree loop guard, 96
 - LAN switching spanning tree port state transition information output, 87
 - LAN switching spanning tree root guard, 95
 - LAN switching spanning tree TC-BPDU guard, 97
 - LLDP for automatic IP phone discovery, 175
 - loop detection (global), 118
 - loop detection (port-specific), 118
 - MAC address move notification, 25
 - MAC address synchronization, 24
 - MAC Information, 30
 - MVRP, 186
 - MVRP GVRP compatibility, 187
 - QinQ, 200
 - SNMP notification for MAC address table, 28
 - spanning tree SNMP notification (new-root election, topology change events), 98
 - speed downgrade autonegotiation (Ethernet interface), 11
 - VLAN mapping M\1 ARP detection (dynamic IP address assignment), 215
 - VLAN mapping M\1 ARP snooping, 217
 - VLAN mapping M\1 DHCP snooping, 215
 - encapsulating
 - L2PT configuration, 107, 109, 111
 - L2PT for LACP configuration, 112
 - L2PT for STP configuration, 111
 - LAN switching LLDP frame encapsulated in Ethernet II, 228
 - LAN switching LLDP frame encapsulated in SNAP format, 228
 - LAN switching LLDP frame encapsulation format, 239
 - VLAN frame encapsulation, 123
 - Energy Efficient Ethernet. *See* EEE
 - energy-saving functions, 5
 - entry
 - ARP fast update enabling for MAC address move, 26
 - Ethernet
 - interface. *See* [Ethernet interface](#)
 - interface auto power-down enable, 5
 - interface basic settings configuration, 2
 - interface display, 12
 - interface EEE energy saving enable, 5
 - interface energy-saving functions, 5
 - interface generic flow control, 4
 - interface jumbo frame support configuration, 2
 - interface loopback test, 4

- interface loopback testing restrictions, 4
- interface maintain, 12
- interface physical state change suppression, 3
- interface statistics polling interval, 6
- LAN switching LLDP frame encapsulated in Ethernet II, 228
- LAN switching LLDP trapping, 242
- LAN switching LLDP-MED trapping, 242
- Layer 2 LAN switching port isolation configuration, 55
- Layer 2 LAN switching port isolation configuration (multiple isolation groups), 56
- link aggregation. See [Ethernet link aggregation](#)
- loop detection configuration, 116, 120
- MAC address table configuration, 17, 18, 28
- MAC Information configuration, 30, 31
- port-based VLAN assignment (access port), 127
- port-based VLAN assignment (hybrid port), 128
- port-based VLAN assignment (trunk port), 128
- private VLAN configuration, 151, 152, 154
- private VLAN promiscuous port configuration, 154
- private VLAN trunk promiscuous port configuration, 157, 160
- private VLAN trunk secondary port configuration, 160
- QinQ CVLAN frame header tag, 198
- QinQ SVLAN frame header tag, 198
- secondary VLAN Layer 3 communication, 165
- super VLAN configuration, 146, 146, 148
- super VLAN sub VLAN configuration, 146
- VLAN basic configuration, 124
- VLAN configuration, 123, 137
- VLAN frame encapsulation, 123
- VLAN interface basics, 125
- VLAN port-based configuration, 126, 137
- voice VLAN automatic assignment mode port operation configuration, 174, 178
- voice VLAN configuration, 168, 178
- voice VLAN interface QoS priority settings configuration, 173
- voice VLAN manual assignment mode port operation configuration, 175, 180

Ethernet interface

- bridging, 11
- combo interface configuration, 1
- common settings configuration, 1
- configuration, 1
- naming conventions, 1

- restrictions for forcibly bringing up fiber ports, 9
- speed downgrade autonegotiation, 11

Ethernet link aggregation

- aggregate group Selected ports min/max, 43
- aggregate interface, 34
- aggregate interface (description), 42
- aggregate interface configuration, 42
- aggregate interface default settings, 45
- aggregate interface shutdown, 45
- aggregation group, 34
- aggregation group restrictions, 41
- basic concepts, 34
- BFD configuration, 44
- configuration, 34, 40, 48
- configuration types, 35
- display, 48
- dynamic mode, 37
- group configuration, 41
- group configuration (dynamic), 42
- group configuration (static), 41
- group load sharing configuration, 46
- group load sharing mode, 46
- how dynamic link aggregation works, 38
- interface configuration (expected bandwidth), 44
- LACP, 37
- Layer 2 aggregate interface (ignored VLAN), 43, 43
- Layer 2 aggregation configuration (dynamic), 50
- Layer 2 aggregation configuration (static), 48
- Layer 2 aggregation load sharing (Layer 2), 52
- Layer 2 group (dynamic), 42
- Layer 2 group (static), 41
- load sharing mode, 40
- local-first load sharing, 46
- maintain, 48
- member port, 34
- member port state, 34, 36, 39
- modes, 35
- operational key, 34
- reference port, 38
- reference port choice, 36
- static mode, 36
- traffic redirection, 47
- traffic redirection restrictions, 47

Ethernet subinterface

- display, 12
- maintain, 12

external

- interface external loopback test (Ethernet), 4

F

- flow control
 - interface generic flow control (Ethernet), 4
- forcing
 - interface fiber port (Layer 2 Ethernet), 8
- format
 - LAN switching LLDP frame encapsulated in Ethernet II, 228
 - LAN switching LLDP frame encapsulated in SNAP format, 228
 - LAN switching LLDP frame encapsulation format, 239
 - LAN switching LLDP management address encoding format, 238
- forwarding
 - LAN switching MST forwarding port state, 69
 - LAN switching spanning tree forward delay timer, 79
 - LAN switching STP BPDU forwarding, 64
 - LAN switching STP forward delay timer, 65
 - MAC address table unknown frame forwarding rule, 23
- frame
 - interface jumbo frame support (Ethernet), 2
 - loop detection (Ethernet frame header), 116
 - loop detection (inner frame header), 116
 - loop detection interval, 117
 - MAC address learning, 17
 - MAC address table blackhole entry, 20
 - MAC address table configuration, 17, 18, 28
 - MAC address table entry configuration, 19
 - MAC address table multiport unicast entry, 20
 - MAC address table unknown frame forwarding rule, 23
 - MAC Information configuration, 30, 31
 - port-based VLAN frame handling, 126
 - QinQ CVLAN Ethernet frame header tag, 198
 - QinQ implementation, 199
 - QinQ SVLAN Ethernet frame header tag, 198
 - VLAN frame encapsulation, 123

G

- GARP
 - VLAN Registration Protocol. *Use GVRP*
- generic flow control (Ethernet interface), 4
- Generic VLAN Registration Protocol. *Use GVRP*
- global
 - Ethernet link aggregation load sharing mode set, 46
 - loop detection enable, 118
 - loop detection protection action, 119
- group
 - Ethernet link aggregate group Selected ports min/max, 43
 - Ethernet link aggregation, 41
 - Ethernet link aggregation group, 34
 - Ethernet link aggregation group (dynamic), 42
 - Ethernet link aggregation group (Layer 2 dynamic), 42
 - Ethernet link aggregation group (Layer 2 static), 41
 - Ethernet link aggregation group (static), 41
 - Ethernet link aggregation group load sharing, 46
 - Ethernet link aggregation LACP, 37
 - Ethernet link aggregation load sharing mode, 40, 46
 - Ethernet link aggregation member port state, 34

GVRP

- MVRP compatibility, 187

H

- hello
 - LAN switching spanning tree timer, 79
 - LAN switching STP timer, 65
- hybrid port
 - port-based VLAN assignment (hybrid port), 128

I

- ignored VLAN
 - Layer 2 aggregate interface, 43
- implementing
 - 1/1 VLAN mapping, 210, 211
 - 1/2 VLAN mapping, 210, 212
 - 2/2 VLAN mapping, 210, 212
 - LAN switching MSTP device implementation, 71
 - M/1 VLAN mapping, 210, 211
 - QinQ, 199
- inloopback interface
 - configuration, 14
 - displaying, 14
 - maintaining, 14
- interface
 - bulk configuration, 15
 - Ethernet aggregate interface, 42
 - Ethernet aggregate interface (description), 42
 - Ethernet link aggregate interface default settings, 45
 - Ethernet link aggregate interface shutdown, 45
 - inloopback configuration, 13, 14
 - Layer 2 Ethernet aggregate interface (ignored VLAN), 43
 - loopback configuration, 13, 13
 - null configuration, 13, 13
- internal

- interface internal loopback test (Ethernet), 4
- interval
 - Ethernet link aggregation LACP long timeout, 38
 - Ethernet link aggregation LACP short timeout, 38
 - loop detection, 117, 119
 - MAC change notification interval, 31
- IP addressing
 - super VLAN configuration, 146, 146, 148
 - super VLAN interface configuration, 147
 - voice VLAN automatic assignment mode port operation configuration, 174, 178
 - voice VLAN configuration, 168, 178
 - voice VLAN interface QoS priority settings configuration, 173
 - voice VLAN manual assignment mode port operation configuration, 175, 180
- IP phone
 - voice VLAN IP phone access method, 170
- IP subnet-based VLAN
 - configuration, 134, 141
- isolating
 - ports. See [port isolation](#)
- IST
 - MST region, 68
- J**
- jumbo frame support (Ethernet interface), 2
- K**
- key
 - Ethernet link aggregation operational key, 34
- L**
- L2PT
 - configuration, 107, 109, 111
 - display, 110
 - enable, 109, 109
 - how it works, 108
 - LACP configuration, 112
 - maintain, 110
 - STP configuration, 111
 - tunneled packet destination multicast MAC address, 110
- LACP
 - Ethernet link aggregation, 37
 - L2PT for LACP configuration, 112
- LAN
 - Virtual Local Area Network. Use [VLAN](#)
- LAN switching
 - displaying LLDP, 242
 - displaying spanning tree, 99
 - Ethernet aggregate interface, 42
 - Ethernet aggregate interface (description), 42
 - Ethernet aggregate interface (ignored VLAN), 43
 - Ethernet link aggregate group Selected ports min/max, 43
 - Ethernet link aggregate interface (expected bandwidth), 44
 - Ethernet link aggregate interface default settings, 45
 - Ethernet link aggregate interface shutdown, 45
 - Ethernet link aggregation (dynamic mode), 37
 - Ethernet link aggregation (Layer 2 dynamic), 50
 - Ethernet link aggregation (Layer 2 static), 48
 - Ethernet link aggregation (static mode), 36
 - Ethernet link aggregation basic concepts, 34
 - Ethernet link aggregation configuration, 34, 40, 48
 - Ethernet link aggregation display, 48
 - Ethernet link aggregation group, 41
 - Ethernet link aggregation group (dynamic dynamic), 42
 - Ethernet link aggregation group (Layer 2 static), 41
 - Ethernet link aggregation group load sharing, 46
 - Ethernet link aggregation group load sharing mode, 46
 - Ethernet link aggregation group restrictions, 41
 - Ethernet link aggregation LACP, 37
 - Ethernet link aggregation load sharing (Layer 2), 52
 - Ethernet link aggregation load sharing mode, 40
 - Ethernet link aggregation local-first load sharing, 46
 - Ethernet link aggregation maintain, 48
 - Ethernet link aggregation traffic redirection, 47
 - Ethernet link aggregation traffic redirection restrictions, 47
 - L2PT configuration, 107, 111
 - L2PT display, 110
 - L2PT for LACP configuration, 112
 - L2PT for STP configuration, 111
 - L2PT maintain, 110
 - LLDP basic concepts, 228
 - LLDP basic configuration, 234, 243
 - LLDP CDP compatibility, 240
 - LLDP configuration, 228, 234, 243
 - LLDP configuration (CDP-compatible), 247
 - maintaining spanning tree, 99
 - MST region, 75
 - MSTP configuration, 100
 - PVST configuration, 103
 - spanning tree configuration, 58, 100

Layer 2

- configuring MAC-based VLAN dynamic assignment, [133](#)
- configuring MAC-based VLAN static assignment, [132](#)
- configuring server-assigned MAC-based VLAN, [133](#)
- Ethernet link aggregation (Layer 2 dynamic), [50](#)
- Ethernet link aggregation (Layer 2 static), [48](#)
- Ethernet link aggregation load sharing, [52](#)
- interface configuration (Ethernet), [1](#)
- interface storm suppression (Ethernet), [6](#)
- L2PT configuration, [109](#)
- L2PT tunneled packet destination multicast MAC address, [110](#)
- LAN switching LLDP basic configuration, [243](#)
- LAN switching LLDP configuration, [243](#)
- LAN switching LLDP trapping, [242](#)
- LAN switching LLDP-MED trapping, [242](#)
- loop detection configuration, [116](#), [118](#), [120](#)
- MAC-based VLAN configuration, [129](#)
- MAC-based VLAN dynamic assignment, [130](#)
- MAC-based VLAN static assignment, [129](#)
- protocol tunneling. *Use* [L2PT](#)
- server-assigned MAC-based VLAN, [131](#)
- voice VLAN automatic assignment mode port operation configuration, [174](#), [178](#)
- voice VLAN configuration, [168](#), [178](#)
- voice VLAN interface QoS priority settings configuration, [173](#)
- voice VLAN manual assignment mode port operation configuration, [175](#), [180](#)

Layer 2 Ethernet

- interface cable connection, [10](#)
- interface fiber port, [8](#)
- interface MDIX mode, [10](#)
- interface storm control configuration, [7](#)

Layer 2 LAN switching

- basic QinQ configuration, [204](#)
- displaying private VLAN, [154](#)
- displaying VLAN, [137](#)
- Ethernet link aggregation group (dynamic), [42](#)
- Ethernet link aggregation group (static), [41](#)
- IP subnet-based VLAN configuration, [134](#), [141](#)
- MAC-based VLAN configuration, [139](#)
- maintaining VLAN, [137](#)
- MRP implementation, [182](#)
- MVRP configuration, [182](#), [185](#), [188](#)
- MVRP GVRP compatibility, [187](#)
- port isolation configuration, [55](#)

- port isolation configuration (multiple isolation groups), [56](#)
- port isolation group assignment (multiple), [55](#)
- port-based VLAN assignment (access port), [127](#)
- port-based VLAN assignment (hybrid port), [128](#)
- port-based VLAN assignment (trunk port), [128](#)
- private VLAN configuration, [151](#), [152](#), [154](#)
- private VLAN promiscuous port configuration, [154](#)
- private VLAN trunk promiscuous port configuration, [157](#), [160](#)
- private VLAN trunk secondary port configuration, [160](#)
- protocol-based VLAN configuration, [135](#), [142](#)
- QinQ configuration, [204](#)
- QinQ implementation, [199](#)
- QinQ SVLAN tag 802.1p priority, [202](#)
- QinQ VLAN tag TPID value, [201](#)
- secondary VLAN Layer 3 communication, [165](#)
- super VLAN configuration, [146](#), [146](#), [148](#)
- super VLAN interface configuration, [147](#)
- super VLAN sub VLAN configuration, [146](#)
- VLAN basic configuration, [124](#)
- VLAN configuration, [123](#), [137](#)
- VLAN group configuration, [136](#)
- VLAN interface basics, [125](#)
- VLAN mapping configuration (1\1), [220](#)
- VLAN mapping configuration, [208](#), [213](#), [220](#)
- VLAN mapping configuration (1\1), [214](#)
- VLAN mapping configuration (1\2), [218](#), [224](#)
- VLAN mapping configuration (2\2), [219](#), [224](#)
- VLAN mapping configuration (M\1), [214](#), [220](#)
- VLAN mapping configuration (M\1) (dynamic IP address assignment), [215](#)
- VLAN mapping configuration (M\1) (static IP address assignment), [217](#)
- VLAN port-based configuration, [126](#), [137](#)

Layer 3

- IP subnet-based VLAN configuration, [134](#), [141](#)
- LAN switching LLDP basic configuration, [243](#)
- LAN switching LLDP configuration, [243](#)
- LAN switching LLDP trapping, [242](#)
- LAN switching LLDP-MED trapping, [242](#)
- LAN switching VLAN interface basics, [125](#)
- MAC-based VLAN configuration, [139](#)
- port-based VLAN assignment (access port), [127](#)
- port-based VLAN assignment (hybrid port), [128](#)
- port-based VLAN assignment (trunk port), [128](#)
- private VLAN configuration, [154](#)
- private VLAN promiscuous port configuration, [154](#)
- private VLAN trunk promiscuous port configuration, [157](#), [160](#)

- private VLAN trunk secondary port configuration, [160](#)
- protocol-based VLAN configuration, [135](#), [142](#)
- secondary VLAN Layer 3 communication, [165](#)
- super VLAN configuration, [148](#)
- VLAN configuration, [137](#)
- VLAN port-based configuration, [126](#), [137](#)
- voice VLAN automatic assignment mode port operation configuration, [174](#), [178](#)
- voice VLAN configuration, [168](#), [178](#)
- voice VLAN interface QoS priority settings configuration, [173](#)
- voice VLAN manual assignment mode port operation configuration, [175](#), [180](#)
- learning
 - LAN switching MST learning port state, [69](#)
 - loop detection no-learning action, [117](#)
 - MAC address, [17](#)
 - MAC address learning disable, [21](#)
- legacy
 - LAN switching spanning tree port mode, [86](#)
 - LAN switching spanning tree port path cost calculation, [82](#)
- link
 - aggregation. See [link aggregation](#)
 - LAN switching MSTP configuration, [100](#)
 - LAN switching PVST configuration, [103](#)
 - LAN switching spanning tree configuration, [58](#), [71](#), [100](#)
 - LAN switching spanning tree hello time, [79](#)
 - LAN switching spanning tree port link type configuration, [85](#)
 - link layer discovery protocol. Use [LLDP](#)
- link aggregation
 - Ethernet link aggregation. See [Ethernet link aggregation](#)
- LLDP
 - advertisable TLV configuration, [237](#)
 - advertising authorization VLANs through LLDP dynamically, [177](#)
 - advertising voice VLAN information to IP phones, [169](#)
 - agent, [228](#)
 - automatically identifying IP phones through LLDP, [169](#)
 - basic concepts, [228](#)
 - basic configuration, [234](#), [243](#)
 - bridge mode configuration, [235](#)
 - CDP compatibility configuration, [240](#)
 - CDP-compatible configuration, [247](#)
 - configuration, [228](#), [234](#), [243](#)
 - configuring LLDP/CDP to advertise a voice VLAN, [176](#)
 - disabling PVID inconsistency check, [240](#)
 - displaying, [242](#)
 - enable, [234](#)
 - enabling LLDP for automatic IP phone discovery, [175](#)
 - how it works, [233](#)
 - LAN switching LLDP-MED trapping configuration, [242](#)
 - LLDP frame encapsulation format, [239](#)
 - LLDP frame format, [228](#)
 - LLDP frame reception, [233](#)
 - LLDP frame transmission, [233](#)
 - LLDPDU management address TLV, [233](#)
 - LLDPDU TLV types, [230](#)
 - LLDPDU TLVs, [230](#)
 - management address configuration, [238](#)
 - management address encoding format, [238](#)
 - methods of identifying IP phones, [168](#)
 - operating mode (disable), [233](#)
 - operating mode (Rx), [233](#)
 - operating mode (Tx), [233](#)
 - operating mode (TxRx), [233](#)
 - operating mode set, [235](#)
 - parameter set, [239](#)
 - polling enable, [236](#)
 - protocols and standards, [234](#)
 - reinitialization delay, [236](#)
 - trapping configuration, [242](#)
- LLDP frame
 - encapsulated in Ethernet II format, [228](#)
 - encapsulated in SNAP format, [228](#)
 - encapsulation format, [239](#)
 - receiving, [233](#)
 - transmitting, [233](#)
- LLDPDU
 - LAN switching LLDP basic configuration, [243](#)
 - LAN switching LLDP configuration, [234](#), [243](#)
 - LLDP basic configuration, [234](#)
 - LLDP configuration, [228](#)
 - LLDP parameters, [239](#)
 - management address configuration, [238](#)
 - management address encoding format, [238](#)
 - management address TLV, [233](#)
 - TLV basic management types, [230](#)
 - TLV LLDP-MED types, [230](#)
 - TLV organization-specific types, [230](#)
- load sharing
 - Ethernet link aggregation group configuration, [46](#)
 - Ethernet link aggregation group load sharing, [40](#)

- Ethernet link aggregation load sharing (Layer 2), [52](#)
- Ethernet link aggregation load sharing mode, [46](#)
- Ethernet link aggregation local-first load sharing, [46](#)
- Ethernet link aggregation packet type-based load sharing, [40](#)
- Ethernet link aggregation per-flow load sharing, [40](#)
- Ethernet link aggregation per-packet load sharing, [40](#)
- local
 - Ethernet link aggregation local-first load sharing, [46](#)
- loop
 - LAN switching MSTP configuration, [100](#)
 - LAN switching PVST configuration, [103](#)
 - LAN switching spanning tree configuration, [58](#), [71](#), [100](#)
 - LAN switching spanning tree loop guard, [96](#)
- loop detection
 - configuration, [116](#), [118](#), [120](#)
 - display, [120](#)
 - enable, [118](#)
 - enable (port-specific), [118](#)
 - interval, [117](#)
 - interval setting, [119](#)
 - mechanisms, [116](#)
 - port status auto recovery, [117](#)
 - protection action configuration, [119](#)
 - protection action configuration (global), [119](#)
 - protection action configuration (Layer 2 aggregate interface), [119](#)
 - protection action configuration (Layer 2 Ethernet interface), [119](#)
 - protection actions, [117](#)
- loopback
 - interface loopback test (Ethernet), [4](#)
- loopback interface
 - configuration, [13](#)
 - displaying, [14](#)
 - maintaining, [14](#)
- M**
- M\
 - 1 VLAN mappingapplication scenario, [208](#)
 - 1 VLAN mappingARP detection (dynamic IP address assignment), [215](#)
 - 1 VLAN mappingARP snooping (static IP address assignment), [217](#)
 - 1 VLAN mappingconfiguration, [214](#), [220](#)
 - 1 VLAN mappingconfiguration (dynamic IP address assignment), [215](#)
 - 1 VLAN mappingconfiguration (static IP address assignment), [217](#)
 - 1 VLAN mappingcustomer-side port (dynamic IP address assignment), [216](#)
 - 1 VLAN mappingcustomer-side port (static IP address assignment), [217](#)
 - 1 VLAN mappingDHCP snooping (dynamic IP address assignment), [215](#)
 - 1 VLAN mappingimplementation, [210](#), [211](#)
 - 1 VLAN mappingnetwork-side port (dynamic IP address assignment), [216](#)
 - 1 VLAN mappingnetwork-side port (static IP address assignment), [218](#)
- MAC address
 - configuring MAC-based VLAN dynamic assignment, [133](#)
 - configuring MAC-based VLAN static assignment, [132](#)
 - configuring server-assigned MAC-based VLAN, [133](#)
 - identifying IP phones through OUI address, [168](#)
 - MAC-based VLAN configuration, [129](#)
 - MAC-based VLAN dynamic assignment, [130](#)
 - MAC-based VLAN static assignment, [129](#)
 - server-assigned MAC-based VLAN, [131](#)
- MAC address move
 - ARP fast update enabling, [26](#)
- MAC address table
 - address learning, [17](#)
 - address synchronization, [24](#)
 - blackhole entry, [20](#)
 - configuration, [17](#), [18](#), [28](#)
 - displaying, [28](#)
 - dynamic aging timer, [22](#)
 - enabling SNMP notification, [28](#)
 - entry configuration, [19](#)
 - entry creation, [17](#)
 - entry types, [17](#)
 - MAC address learning disable, [21](#)
 - MAC address move notification, [25](#)
 - manual entries, [17](#)
 - multiport unicast entry, [20](#)
 - static source check disable, [27](#)
 - unknown frame forwarding rule, [23](#)
- MAC address table learning limit on interface configuration, [23](#)
- MAC addressing
 - L2PT tunneled packet destination multicast MAC address, [110](#)
 - MAC-based VLAN configuration, [139](#)

- VLAN frame encapsulation, [123](#)
- MAC Information
 - change notification interval, [31](#)
 - configuration, [30, 31](#)
 - enable, [30](#)
 - mode configuration, [30](#)
 - queue length configuration, [31](#)
- MAC relay (LLDP agent), [228](#)
- MAC-based
 - configuration, [139](#)
- MAC-based VLAN
 - configuration, [129](#)
 - configuring dynamic assignment, [133](#)
 - configuring server-assigned MAC-based VLAN, [133](#)
 - configuring static assignment, [132](#)
 - dynamic assignment, [130](#)
 - server-assigned, [131](#)
 - static assignment, [129](#)
- maintaining
 - Ethernet link aggregation, [48](#)
 - interface, [14](#)
 - interface (Ethernet), [12](#)
 - L2PT, [110](#)
 - LAN switching spanning tree, [99](#)
 - MVRP, [188](#)
 - subinterface (Ethernet), [12](#)
 - VLAN, [137](#)
- management address
 - LAN switching LLDP encoding format, [238](#)
- manual
 - voice VLAN assignment mode, [171](#)
 - voice VLAN automatic assignment mode port operation configuration, [180](#)
 - voice VLAN manual assignment mode port operation configuration, [175](#)
- mapping
 - 111 VLAN mapping, [208](#)
 - 112 VLAN mapping, [210](#)
 - 212 VLAN mapping, [210](#)
 - LAN switching MSTP VLAN-to-instance mapping table, [68](#)
 - M11 VLAN mapping, [208](#)
- master port (MST), [69](#)
- max age timer (STP), [65](#)
- mCheck
 - LAN switching global performance, [88](#)
 - LAN switching interface view performance, [89](#)
 - LAN switching spanning tree, [88](#)
- MDI mode (Ethernet interface), [10](#)
- MDIX mode (Ethernet interface), [10](#)
- MED (LLDP-MED trapping), [242](#)
- message
 - MRP JoinEmpty, [182](#)
 - MRP JoinIn, [182](#)
 - MRP Leave, [182](#)
 - MRP LeaveAll, [182](#)
 - MRP New, [182](#)
 - MRP timers, [184](#)
- MIB
 - LAN switching LLDP basic configuration, [234, 243](#)
 - LAN switching LLDP configuration, [228, 234, 243](#)
- mode
 - Ethernet link aggregation dynamic, [35, 37](#)
 - Ethernet link aggregation load sharing, [40](#)
 - Ethernet link aggregation static, [35, 36](#)
 - interface Auto MDIX mode (Layer 2 Ethernet), [10](#)
 - interface MDI mode (Layer 2 Ethernet), [10](#)
 - interface MDIX mode (Layer 2 Ethernet), [10](#)
 - LAN switching LLDP customer bridge mode, [235](#)
 - LAN switching LLDP disable, [233, 235](#)
 - LAN switching LLDP Rx, [233, 235](#)
 - LAN switching LLDP service bridge mode, [235](#)
 - LAN switching LLDP Tx, [233, 235](#)
 - LAN switching LLDP TxRx, [233, 235](#)
 - LAN switching spanning tree mCheck, [88](#)
 - LAN switching spanning tree MSTP mode, [74](#)
 - LAN switching spanning tree PVST mode, [74](#)
 - LAN switching spanning tree RSTP mode, [74](#)
 - LAN switching spanning tree STP mode, [74](#)
 - MAC Information syslog, [30](#)
 - MAC Information trap, [30](#)
 - MVRP registration fixed mode, [184](#)
 - MVRP registration forbidden mode, [184](#)
 - MVRP registration mode, [186](#)
 - MVRP registration normal mode, [184](#)
 - voice VLAN automatic assignment mode, [170](#)
 - voice VLAN automatic assignment mode port operation configuration, [174, 178](#)
 - voice VLAN manual assignment mode, [171](#)
 - voice VLAN manual assignment mode port operation configuration, [175, 180](#)
 - voice VLAN normal mode, [172](#)
 - voice VLAN security mode, [172](#)
- modifying
 - MAC address table blackhole entry, [20](#)
 - MAC address table multiport unicast entry, [20](#)
- MRP
 - implementation, [182](#)
 - messages, [182](#)
 - MVRP configuration, [182, 185, 188](#)

- timers, [184](#)
- MST
 - region max hops, [78](#)
- MSTI
 - calculation, [70](#)
 - MRP, [182](#)
 - MST instance, [68](#)
- MSTP, [58](#), *See also* [STP](#)
 - basic concepts, [66](#)
 - CIST, [68](#)
 - CIST calculation, [70](#)
 - common root bridge, [68](#)
 - configuration, [74](#), [100](#)
 - CST, [68](#)
 - device implementation, [71](#)
 - feature enable, [87](#)
 - features, [66](#)
 - how it works, [70](#)
 - IST, [68](#)
 - mode set, [74](#)
 - MST region, [67](#)
 - MST region configuration, [75](#)
 - MSTI, [68](#)
 - MSTI calculation, [70](#)
 - port roles, [69](#)
 - port states, [69](#)
 - protocols and standards, [71](#)
 - regional root, [68](#)
 - relationships, [66](#)
 - spanning tree max age timer, [79](#)
 - spanning tree port mode configuration, [86](#)
 - VLAN-to-instance mapping table, [68](#)
- multicast
 - L2PT tunneled packet destination multicast MAC address, [110](#)
- multiple
 - Registration Protocol. *Use* [MRP](#)
 - VLAN Registration Protocol. *Use* [MVRP](#)
- Multiple Spanning Tree Protocol. *Use* [MSTP](#)
- multiport unicast entry (MAC address table), [17](#), [20](#)
- MVRP
 - configuration, [182](#), [185](#), [188](#)
 - configuration restrictions, [185](#)
 - displaying, [188](#)
 - enable, [186](#)
 - GVRP compatibility, [187](#)
 - maintaining, [188](#)
 - MRP implementation, [182](#)
 - protocols and standards, [185](#)
 - registration mode configuration, [186](#)

- registration modes, [184](#)
- timer configuration, [187](#)

N

- network
 - Ethernet link aggregation (dynamic mode), [37](#)
 - Ethernet link aggregation (Layer 2 dynamic), [50](#)
 - Ethernet link aggregation (Layer 2 static), [48](#)
 - Ethernet link aggregation (static mode), [36](#)
 - Ethernet link aggregation configuration types, [35](#)
 - Ethernet link aggregation LACP, [37](#)
 - Ethernet link aggregation load sharing (Layer 2), [52](#)
 - Ethernet link aggregation member port state, [36](#), [39](#)
 - Ethernet link aggregation modes, [35](#)
 - Ethernet link aggregation operational key, [34](#)
 - Ethernet link aggregation reference port, [38](#)
 - Ethernet link aggregation reference port choice, [36](#)
 - inloopback interface configuration, [14](#)
 - interface auto power-down (Ethernet), [5](#)
 - interface basic settings (Ethernet), [2](#)
 - interface cable connection (Layer 2 Ethernet), [10](#)
 - interface common settings configuration (Ethernet), [1](#)
 - interface configuration (Ethernet combo), [1](#)
 - interface EEE energy saving, [5](#)
 - interface energy-saving functions (Ethernet), [5](#)
 - interface fiber port (Layer 2 Ethernet), [8](#)
 - interface generic flow control (Ethernet), [4](#)
 - interface jumbo frame support (Ethernet), [2](#)
 - interface loopback test (Ethernet), [4](#)
 - interface MDIX mode (Layer 2 Ethernet), [10](#)
 - interface physical state change suppression (Ethernet), [3](#)
 - interface statistics polling interval (Ethernet), [6](#)
 - interface storm control (Layer 2 Ethernet), [7](#)
 - interface storm suppression (Layer 2 Ethernet), [6](#)
 - L2PT enable, [109](#)
 - L2PT for LACP configuration, [112](#)
 - L2PT for STP configuration, [111](#)
 - L2PT tunneled packet destination multicast MAC address, [110](#)
 - LAN switching LLDP basic configuration, [234](#)
 - LAN switching MST region configuration, [75](#)
 - LAN switching RSTP network convergence, [65](#)
 - LAN switching spanning tree BPDU drop, [98](#)
 - LAN switching spanning tree BPDU guard, [95](#)
 - LAN switching spanning tree BPDU transmission rate, [80](#)

- LAN switching spanning tree Digest Snooping, [89](#), [90](#)
- LAN switching spanning tree edge port, [81](#)
- LAN switching spanning tree loop guard, [96](#)
- LAN switching spanning tree mode set, [74](#)
- LAN switching spanning tree No Agreement Check, [91](#), [93](#)
- LAN switching spanning tree port link type, [85](#)
- LAN switching spanning tree port mode, [86](#)
- LAN switching spanning tree port path cost, [81](#), [84](#)
- LAN switching spanning tree port priority, [85](#)
- LAN switching spanning tree port role restriction, [96](#)
- LAN switching spanning tree port state transition, [87](#)
- LAN switching spanning tree priority, [77](#)
- LAN switching spanning tree protection functions, [94](#)
- LAN switching spanning tree root bridge, [76](#)
- LAN switching spanning tree root bridge (device), [77](#)
- LAN switching spanning tree root guard, [95](#)
- LAN switching spanning tree secondary root bridge (device), [77](#)
- LAN switching spanning tree switched network diameter, [78](#)
- LAN switching spanning tree TC Snooping, [93](#)
- LAN switching spanning tree TC-BPDU guard, [97](#)
- LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
- LAN switching STP algorithm calculation, [60](#)
- LAN switching STP designated bridge, [59](#)
- LAN switching STP designated port, [59](#)
- LAN switching STP path cost, [60](#)
- LAN switching STP root bridge, [59](#)
- LAN switching STP root port, [59](#)
- Layer 2 LAN switching port isolation group assignment (multiple), [55](#)
- loop detection enable, [118](#)
- loop detection interval, [117](#), [119](#)
- loop detection protection action configuration, [119](#)
- loop protection actions, [117](#)
- loopback interface configuration, [13](#)
- MAC address move notification, [25](#)
- MAC address table address synchronization, [24](#)
- MAC address table blackhole entry, [20](#)
- MAC address table dynamic aging timer, [22](#)
- MAC address table entry configuration, [19](#)
- MAC address table entry types, [17](#)
- MAC address table multiport unicast entry, [20](#)
- MRP timers, [184](#)
- MVRP timer configuration, [187](#)
- null interface configuration, [13](#)
- port-based VLAN assignment (access port), [127](#)
- port-based VLAN assignment (hybrid port), [128](#)
- port-based VLAN assignment (trunk port), [128](#)
- QinQ CVLAN tag TPID value, [202](#)
- QinQ SVLAN tag TPID value, [202](#)
- QinQ VLAN tag TPID value, [201](#)
- QinQ VLAN transparent transmission, [200](#)
- SNMP notification for MAC address table, [28](#)
- spanning tree SNMP notification (new-root election, topology change events), [98](#)
- super VLAN configuration, [146](#)
- super VLAN interface configuration, [147](#)
- super VLAN sub VLAN configuration, [146](#)
- VLAN basic configuration, [124](#)
- VLAN configuration, [137](#)
- VLAN group configuration, [136](#)
- VLAN interface basics, [125](#)
- VLAN mapping 1\1 implementation, [211](#)
- VLAN mapping 1\2 implementation, [212](#)
- VLAN mapping 2\2 implementation, [212](#)
- VLAN mapping configuration (1\1), [214](#)
- VLAN mapping configuration (1\2), [218](#)
- VLAN mapping configuration (2\2), [219](#)
- VLAN mapping configuration (M\1), [214](#)
- VLAN mapping configuration (M\1) (dynamic IP address assignment), [215](#)
- VLAN mapping configuration (M\1) (static IP address assignment), [217](#)
- VLAN mapping M\1 customer-side port (dynamic IP address assignment), [216](#)
- VLAN mapping M\1 customer-side port (static IP address assignment), [217](#)
- VLAN mapping M\1 implementation, [211](#)
- VLAN mapping M\1 network-side port (dynamic IP address assignment), [216](#)
- VLAN mapping M\1 network-side port (static IP address assignment), [218](#)
- VLAN port-based configuration, [126](#), [137](#)
- voice VLAN IP phone access method, [170](#)
- network management
 - basic QinQ configuration, [204](#)
 - configuring MAC-based VLAN dynamic assignment, [133](#)
 - configuring MAC-based VLAN static assignment, [132](#)
 - configuring server-assigned MAC-based VLAN, [133](#)

- connecting host and IP phone in series, [170](#)
- connecting IP phone to device, [170](#)
- Ethernet link aggregation basic concepts, [34](#)
- Ethernet link aggregation configuration, [34](#), [40](#), [48](#)
- inloopback interface configuration, [13](#)
- interface bulk configuration, [15](#)
- interface configuration (Ethernet), [1](#)
- IP subnet-based VLAN configuration, [134](#), [141](#)
- L2PT configuration, [107](#), [109](#), [111](#)
- LAN switching LLDP basic concepts, [228](#)
- LAN switching LLDP basic configuration, [243](#)
- LAN switching LLDP configuration, [228](#), [234](#), [243](#)
- LAN switching LLDP configuration (CDP-compatible), [247](#)
- LAN switching MSTP configuration, [100](#)
- LAN switching PVST configuration, [103](#)
- LAN switching spanning tree configuration, [58](#), [71](#), [100](#)
- Layer 2 LAN switching port isolation configuration, [55](#)
- Layer 2 LAN switching port isolation configuration (multiple isolation groups), [56](#)
- loop detection, [116](#)
- loop detection configuration, [118](#), [120](#)
- loopback interface configuration, [13](#)
- MAC address table configuration, [17](#), [18](#), [28](#)
- MAC Information configuration, [30](#), [31](#)
- MAC-based VLAN configuration, [129](#), [139](#)
- MAC-based VLAN dynamic assignment, [130](#)
- MAC-based VLAN static assignment, [129](#)
- MVRP, [182](#), [185](#), [188](#)
- null interface configuration, [13](#)
- private VLAN configuration, [151](#), [152](#), [154](#)
- private VLAN promiscuous port configuration, [154](#)
- private VLAN trunk promiscuous port configuration, [157](#), [160](#)
- private VLAN trunk secondary port configuration, [160](#)
- protocol-based VLAN configuration, [135](#), [142](#)
- QinQ configuration, [198](#), [204](#)
- QinQ VLAN transparent transmission configuration, [206](#)
- secondary VLAN Layer 3 communication, [165](#)
- server-assigned MAC-based VLAN, [131](#)
- super VLAN configuration, [146](#), [148](#)
- VLAN configuration, [123](#)
- VLAN mapping configuration, [208](#), [213](#), [220](#)
- VLAN mapping configuration (1\1), [220](#)

- VLAN mapping configuration (1\2), [224](#)
- VLAN mapping configuration (2\2), [224](#)
- VLAN mapping configuration (M1), [220](#)
- voice VLAN automatic assignment mode port operation configuration, [174](#), [178](#)
- voice VLAN configuration, [168](#), [178](#)
- voice VLAN interface QoS priority settings configuration, [173](#)
- voice VLAN manual assignment mode port operation configuration, [175](#), [180](#)
- No Agreement Check (spanning tree), [91](#), [93](#)
- no-learning action (loop detection), [117](#)
- normal
 - voice VLAN mode, [172](#)
- notification
 - MAC address move, [25](#)
 - SNMP notification for MAC address table, [28](#)
- null interface
 - configuration, [13](#), [13](#)
 - displaying, [14](#)
 - maintaining, [14](#)
- O**
- operational key (Ethernet link aggregation), [34](#)
- organization-specific LLDPDU TLV types, [230](#)
- OUI address
 - identifying IP phones through OUI address, [168](#)
 - methods of identifying IP phones, [168](#)
- outputting
 - LAN switching spanning tree port state transition information, [87](#)
- P**
- packet
 - Ethernet link aggregation group BFD, [44](#)
 - Ethernet link aggregation packet type-based load sharing, [40](#)
 - L2PT configuration, [107](#), [109](#), [111](#)
 - L2PT for LACP configuration, [112](#)
 - L2PT for STP configuration, [111](#)
 - L2PT tunneled packet destination multicast MAC address, [110](#)
 - LAN switching LLDP CDP compatibility, [240](#)
 - LAN switching spanning tree port mode configuration, [86](#)
 - LAN switching STP BPDU protocol packets, [58](#)
 - LAN switching STP TCN BPDU protocol packets, [58](#)
 - VLAN mapping configuration, [208](#), [213](#), [220](#)
 - VLAN mapping configuration (1\1), [214](#), [220](#)
 - VLAN mapping configuration (1\2), [218](#), [224](#)
 - VLAN mapping configuration (2\2), [219](#), [224](#)

- VLAN mapping configuration (M1), [214](#), [220](#)
- VLAN mapping configuration (M1) (dynamic IP address assignment), [215](#)
- VLAN mapping configuration (M1) (static IP address assignment), [217](#)
- parameter
 - LAN switching spanning tree timeout factor, [80](#)
- PE
 - L2PT configuration, [107](#), [109](#), [111](#)
 - L2PT for LACP configuration, [112](#)
 - L2PT for STP configuration, [111](#)
- per-flow load sharing, [40](#)
- performing
 - interface loopback test (Ethernet), [4](#)
 - LAN switching spanning tree mCheck, [88](#)
 - LAN switching spanning tree mCheck in interface view, [89](#)
 - spanning tree mCheck globally, [88](#)
- per-packet load sharing, [40](#)
- Per-VLAN Spanning Tree Protocol. Use [PVST](#)
- physical
 - interface physical state change suppression (Ethernet), [3](#)
- polling
 - LAN switching LLDP enable, [236](#)
- polling interval, [6](#)
- port
 - Ethernet aggregate interface, [42](#)
 - Ethernet aggregate interface (description), [42](#)
 - Ethernet link aggregate group Selected ports min/max, [43](#)
 - Ethernet link aggregate interface (expected bandwidth), [44](#)
 - Ethernet link aggregate interface default settings, [45](#)
 - Ethernet link aggregate interface shutdown, [45](#)
 - Ethernet link aggregation (dynamic mode), [37](#)
 - Ethernet link aggregation (Layer 2 dynamic), [50](#)
 - Ethernet link aggregation (Layer 2 static), [48](#)
 - Ethernet link aggregation (static mode), [36](#)
 - Ethernet link aggregation configuration, [34](#), [40](#), [48](#)
 - Ethernet link aggregation configuration types, [35](#)
 - Ethernet link aggregation group, [41](#)
 - Ethernet link aggregation group (dynamic), [42](#)
 - Ethernet link aggregation group (Layer 2 dynamic), [42](#)
 - Ethernet link aggregation group (Layer 2 static), [41](#)
 - Ethernet link aggregation group (static), [41](#)
 - Ethernet link aggregation group load sharing, [46](#)
 - Ethernet link aggregation LACP, [37](#)
 - Ethernet link aggregation LACP port priority, [38](#)
 - Ethernet link aggregation load sharing (Layer 2), [52](#)
 - Ethernet link aggregation load sharing mode, [40](#)
 - Ethernet link aggregation local-first load sharing, [46](#)
 - Ethernet link aggregation member port, [34](#)
 - Ethernet link aggregation member port state, [34](#), [36](#), [39](#)
 - Ethernet link aggregation modes, [35](#)
 - Ethernet link aggregation operational key, [34](#)
 - Ethernet link aggregation reference port, [38](#)
 - Ethernet link aggregation reference port choice, [36](#)
 - Ethernet link aggregation traffic redirection, [47](#)
 - interface fiber port (Layer 2 Ethernet), [8](#)
 - isolation. See [port isolation](#)
 - LAN switching LLDP basic configuration, [234](#), [243](#)
 - LAN switching LLDP configuration, [228](#), [234](#), [243](#)
 - LAN switching LLDP disable operating mode, [233](#)
 - LAN switching LLDP enable, [234](#)
 - LAN switching LLDP frame encapsulation format, [239](#)
 - LAN switching LLDP frame reception, [233](#)
 - LAN switching LLDP frame transmission, [233](#)
 - LAN switching LLDP operating mode, [235](#)
 - LAN switching LLDP polling, [236](#)
 - LAN switching LLDP reinitialization delay, [236](#)
 - LAN switching LLDP Rx operating mode, [233](#)
 - LAN switching LLDP Tx operating mode, [233](#)
 - LAN switching LLDP TxRx operating mode, [233](#)
 - LAN switching MST port roles, [69](#)
 - LAN switching MST port states, [69](#)
 - LAN switching RSTP network convergence, [65](#)
 - LAN switching spanning tree BPDU drop, [98](#)
 - LAN switching spanning tree BPDU guard, [95](#)
 - LAN switching spanning tree BPDU transmission rate, [80](#)
 - LAN switching spanning tree edge port configuration, [81](#)
 - LAN switching spanning tree forward delay timer, [79](#)
 - LAN switching spanning tree loop guard, [96](#)
 - LAN switching spanning tree path cost calculation standard, [82](#)

- LAN switching spanning tree path cost configuration, [81](#), [84](#)
- LAN switching spanning tree port link type configuration, [85](#)
- LAN switching spanning tree port mode configuration, [86](#)
- LAN switching spanning tree port priority configuration, [85](#)
- LAN switching spanning tree port role restriction, [96](#)
- LAN switching spanning tree port state transition output, [87](#)
- LAN switching spanning tree root guard, [95](#)
- LAN switching spanning tree TC-BPDU guard, [97](#)
- LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
- LAN switching STP designated port, [59](#)
- LAN switching STP root port, [59](#)
- Layer 2 aggregate interface (ignored VLAN), [43](#)
- loop detection configuration, [116](#), [118](#), [120](#)
- loop detection enable (port-specific), [118](#)
- loop detection interval, [117](#), [119](#)
- loop detection protection action configuration, [119](#)
- loop detection protection actions, [117](#)
- loop detection status auto recovery, [117](#)
- MAC address learning, [17](#)
- MAC address table blackhole entry, [20](#)
- MAC address table configuration, [17](#), [18](#), [28](#)
- MAC address table entry configuration, [19](#)
- MAC address table multiport unicast entry, [20](#)
- MAC Information configuration, [30](#), [31](#)
- MVRP application, [182](#), [185](#), [188](#)
- MVRP timer configuration, [187](#)
- QinQ implementation, [199](#)
- VLAN mapping M₁ customer-side port (dynamic IP address assignment), [216](#)
- VLAN mapping M₁ customer-side port (static IP address assignment), [217](#)
- VLAN mapping M₁ network-side port (dynamic IP address assignment), [216](#)
- VLAN mapping M₁ network-side port (static IP address assignment), [218](#)
- VLAN port link type, [126](#)
- voice VLAN automatic assignment mode port operation configuration, [174](#), [178](#)
- voice VLAN manual assignment mode port operation configuration, [175](#), [180](#)
- port isolation
 - configuration, [55](#)
 - configuration (multiple isolation groups), [56](#)
 - displaying, [55](#)
 - port assignment to group (multiple), [55](#)
- port-based VLAN
 - assignment (access port), [127](#)
 - assignment (hybrid port), [128](#)
 - assignment (trunk port), [128](#)
 - configuration, [126](#), [137](#)
 - port frame handling, [126](#)
 - port link type, [126](#)
 - PVID, [126](#)
- power
 - interface auto power-down (Ethernet), [5](#)
 - interface EEE energy saving, [5](#)
 - interface energy-saving functions (Ethernet), [5](#)
- priority
 - Ethernet link aggregation LACP, [37](#)
 - Ethernet link aggregation LACP port priority, [38](#)
 - Ethernet link aggregation LACP system priority, [38](#)
 - LAN switching spanning tree device priority, [77](#)
 - LAN switching spanning tree port priority configuration, [85](#)
 - QinQ SVLAN tag 802.1p priority, [202](#)
 - voice VLAN interface QoS priority settings configuration, [173](#)
- private VLAN
 - configuration, [151](#), [152](#), [154](#)
 - displaying, [154](#)
 - promiscuous port configuration, [154](#)
 - secondary VLAN Layer 3 communication, [165](#)
 - trunk promiscuous port configuration, [157](#), [160](#)
 - trunk secondary port configuration, [160](#)
- procedure
 - adding MAC address table blackhole entry, [20](#)
 - adding MAC address table multiport unicast entry, [20](#)
 - advertising authorization VLANs through LLDP/CDP dynamically, [177](#)
 - assigning Layer 2 LAN switching port isolation group (multiple), [55](#)
 - assigning port-based VLAN access port (interface view), [127](#)
 - assigning port-based VLAN access port (VLAN view), [127](#)
 - assigning port-based VLAN hybrid port, [128](#)
 - assigning port-based VLAN trunk port, [128](#)
 - bulk configuring interfaces, [15](#)
 - configuring basic QinQ, [204](#)
 - configuring Ethernet aggregate interface, [42](#)
 - configuring Ethernet aggregate interface (description), [42](#)
 - configuring Ethernet link aggregation, [40](#)

configuring Ethernet link aggregation (Layer 2 dynamic), [50](#)
 configuring Ethernet link aggregation (Layer 2 static), [48](#)
 configuring Ethernet link aggregation group, [41](#)
 configuring Ethernet link aggregation group (dynamic), [42](#)
 configuring Ethernet link aggregation group (Layer 2 dynamic), [42](#)
 configuring Ethernet link aggregation group (Layer 2 static), [41](#)
 configuring Ethernet link aggregation group (static), [41](#)
 configuring Ethernet link aggregation group BFD, [44](#)
 configuring Ethernet link aggregation group load sharing, [46](#)
 configuring Ethernet link aggregation load sharing (Layer 2), [52](#)
 configuring interface (Ethernet combo), [1](#)
 configuring interface (inloopback), [14](#)
 configuring interface (loopback), [13](#)
 configuring interface (null), [13](#)
 configuring interface auto power-down (Ethernet), [5](#)
 configuring interface basic settings (Ethernet), [2](#)
 configuring interface common settings (Ethernet), [1](#)
 configuring interface EEE energy saving, [5](#)
 configuring interface energy-saving functions (Ethernet), [5](#)
 configuring interface generic flow control (Ethernet), [4](#)
 configuring interface jumbo frame support (Ethernet), [2](#)
 configuring interface physical state change suppression (Ethernet), [3](#)
 configuring interface storm control (Layer 2 Ethernet), [7](#)
 configuring interface storm suppression (Layer 2 Ethernet), [6](#)
 configuring IP subnet-based VLAN, [134](#), [141](#)
 configuring L2PT, [109](#)
 configuring L2PT for LACP, [112](#)
 configuring L2PT for STP, [111](#)
 configuring LAN switching LLDP, [234](#), [243](#)
 configuring LAN switching LLDP (CDP-compatible), [247](#)
 configuring LAN switching LLDP advertisable TLVs, [237](#)
 configuring LAN switching LLDP basics, [234](#), [243](#)
 configuring LAN switching LLDP bridge mode, [235](#)
 configuring LAN switching LLDP CDP compatibility, [240](#)
 configuring LAN switching LLDP management address, [238](#)
 configuring LAN switching LLDP management address encoding format, [238](#)
 configuring LAN switching LLDP trapping, [242](#)
 configuring LAN switching LLDP-MED trapping, [242](#)
 configuring LAN switching MST region, [75](#)
 configuring LAN switching MST region max hops, [78](#)
 configuring LAN switching MSTP, [74](#), [100](#)
 configuring LAN switching PVST, [73](#), [103](#)
 configuring LAN switching QinQ VLAN tag TPID value, [201](#)
 configuring LAN switching RSTP, [72](#)
 configuring LAN switching spanning tree, [71](#), [100](#)
 configuring LAN switching spanning tree BPDU transmission rate, [80](#)
 configuring LAN switching spanning tree device priority, [77](#)
 configuring LAN switching spanning tree Digest Snooping, [89](#), [90](#)
 configuring LAN switching spanning tree edge port, [81](#)
 configuring LAN switching spanning tree No Agreement Check, [91](#), [93](#)
 configuring LAN switching spanning tree port link type, [85](#)
 configuring LAN switching spanning tree port mode for MSTP packets, [86](#)
 configuring LAN switching spanning tree port path cost, [81](#), [84](#)
 configuring LAN switching spanning tree port priority, [85](#)
 configuring LAN switching spanning tree port role restriction, [96](#)
 configuring LAN switching spanning tree protection functions, [94](#)
 configuring LAN switching spanning tree root bridge, [76](#)
 configuring LAN switching spanning tree root bridge (device), [77](#)
 configuring LAN switching spanning tree secondary root bridge, [76](#)
 configuring LAN switching spanning tree secondary root bridge (device), [77](#)
 configuring LAN switching spanning tree switched network diameter, [78](#)
 configuring LAN switching spanning tree TC Snooping, [93](#)

configuring LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
 configuring LAN switching spanning tree timeout factor, [80](#)
 configuring LAN switching spanning tree timer, [79](#)
 configuring LAN switching STP, [72](#)
 configuring Layer 2 LAN switching port isolation (multiple isolation groups), [56](#)
 configuring LLDP/CDP to advertise a voice VLAN, [176](#)
 configuring loop detection, [118](#), [120](#)
 configuring loop detection protection action, [119](#)
 configuring loop detection protection action (global), [119](#)
 configuring loop detection protection action (Layer 2 aggregate interface), [119](#)
 configuring loop detection protection action (Layer 2 Ethernet interface), [119](#)
 configuring MAC address table, [28](#)
 configuring MAC address table dynamic aging timer, [22](#)
 configuring MAC address table entry, [19](#)
 configuring MAC address table learning limit on interface, [23](#)
 configuring MAC address table unknown frame forwarding rule, [23](#)
 configuring MAC change notification interval, [31](#)
 configuring MAC Information, [31](#)
 configuring MAC Information mode, [30](#)
 configuring MAC Information queue length, [31](#)
 configuring MAC-based VLAN, [133](#), [139](#)
 configuring MAC-based VLAN dynamic assignment, [133](#)
 configuring MAC-based VLAN static assignment, [132](#)
 configuring MVRP, [185](#), [188](#)
 configuring MVRP registration mode, [186](#)
 configuring MVRP timer, [187](#)
 configuring port-based VLAN, [126](#), [137](#)
 configuring private VLAN, [151](#), [152](#), [154](#)
 configuring private VLAN promiscuous port, [154](#)
 configuring private VLAN trunk promiscuous port, [157](#), [160](#)
 configuring private VLAN trunk secondary port, [160](#)
 configuring protocol-based VLAN, [135](#), [142](#)
 configuring QinQ, [204](#)
 configuring QinQ CVLAN tag TPID value, [202](#)
 configuring QinQ SVLAN tag TPID value, [202](#)
 configuring QinQ transparent transmission for VLAN, [200](#)
 configuring QinQ VLAN transparent transmission, [206](#)
 configuring secondary VLAN Layer 3 communication, [165](#)
 configuring super VLAN, [146](#), [148](#)
 configuring super VLAN interface, [147](#)
 configuring super VLAN sub VLAN, [146](#)
 configuring VLAN, [137](#)
 configuring VLAN basic settings, [124](#)
 configuring VLAN group, [136](#)
 configuring VLAN interface basics, [125](#)
 configuring VLAN mapping, [213](#), [220](#)
 configuring VLAN mapping (1\1), [214](#), [220](#)
 configuring VLAN mapping (1\2), [218](#), [224](#)
 configuring VLAN mapping (2\2), [219](#), [224](#)
 configuring VLAN mapping (M\1), [214](#), [220](#)
 configuring VLAN mapping (M\1) (dynamic IP address assignment), [215](#)
 configuring VLAN mapping (M\1) (static IP address assignment), [217](#)
 configuring VLAN mapping M\1 customer-side port (dynamic IP address assignment), [216](#)
 configuring VLAN mapping M\1 customer-side port (static IP address assignment), [217](#)
 configuring VLAN mapping M\1 network-side port (dynamic IP address assignment), [216](#)
 configuring VLAN mapping M\1 network-side port (static IP address assignment), [218](#)
 configuring voice VLAN, [178](#)
 configuring voice VLAN automatic assignment mode port operation, [174](#), [178](#)
 configuring voice VLAN interface QoS priority settings, [173](#)
 configuring voice VLAN manual assignment mode port operation, [175](#), [180](#)
 configuring voice VLAN on a port, [170](#)
 disabling global MAC address learning, [21](#)
 disabling MAC address learning, [21](#)
 disabling MAC address learning on interface, [22](#)
 disabling MAC address learning on VLAN, [22](#)
 disabling PVID inconsistency check, [240](#)
 disabling static source check, [27](#)
 displaying bulk interface configuration, [16](#)
 displaying Ethernet link aggregation, [48](#)
 displaying interface, [14](#)
 displaying interface (Ethernet), [12](#)
 displaying L2PT, [110](#)
 displaying LAN switching LLDP, [242](#)
 displaying LAN switching spanning tree, [99](#)
 displaying Layer 2 LAN switchingport isolation, [55](#)

- displaying loop detection, [120](#)
- displaying MAC address table, [28](#)
- displaying MVRP, [188](#)
- displaying private VLAN, [154](#)
- displaying QinQ, [203](#)
- displaying subinterface (Ethernet), [12](#)
- displaying super VLAN, [147](#)
- displaying VLAN, [137](#)
- displaying VLAN mapping, [220](#)
- displaying voice VLAN, [177](#)
- enabling ARP fast update for MAC address move, [26](#)
- enabling bridging on Ethernet interface, [11](#)
- enabling Ethernet link aggregation local-first load sharing, [46](#)
- enabling Ethernet link aggregation traffic redirection, [47](#)
- enabling L2PT, [109](#), [109](#)
- enabling LAN switching LLDP, [234](#)
- enabling LAN switching LLDP polling, [236](#)
- enabling LAN switching spanning tree BPDU drop, [98](#)
- enabling LAN switching spanning tree BPDU guard, [95](#)
- enabling LAN switching spanning tree feature, [87](#)
- enabling LAN switching spanning tree loop guard, [96](#)
- enabling LAN switching spanning tree port state transition information output, [87](#)
- enabling LAN switching spanning tree root guard, [95](#)
- enabling LAN switching spanning tree TC-BPDU guard, [97](#)
- enabling LLDP for automatic IP phone discovery, [175](#)
- enabling loop detection (global), [118](#)
- enabling loop detection (port-specific), [118](#)
- enabling MAC address move notification, [25](#)
- enabling MAC address synchronization globally, [24](#)
- enabling MAC Information, [30](#)
- enabling MVRP, [186](#)
- enabling MVRP GVRP compatibility, [187](#)
- enabling QinQ, [200](#)
- enabling SNMP notification for MAC address table, [28](#)
- enabling spanning tree SNMP notification (new-root election, topology change events), [98](#)
- enabling speed downgrade autonegotiation on Ethernet interface, [11](#)
- enabling VLAN mapping M1 ARP detection (dynamic IP address assignment), [215](#)
- enabling VLAN mapping M1 ARP snooping (static IP address assignment), [217](#)
- enabling VLAN mapping M1 DHCP snooping (dynamic IP address assignment), [215](#)
- forcing interface fiber port (Layer 2 Ethernet), [8](#)
- maintaining Ethernet link aggregation, [48](#)
- maintaining interface, [14](#)
- maintaining interface (Ethernet), [12](#)
- maintaining L2PT, [110](#)
- maintaining LAN switching spanning tree, [99](#)
- maintaining MVRP, [188](#)
- maintaining subinterface (Ethernet), [12](#)
- maintaining VLAN, [137](#)
- modifying MAC address table blackhole entry, [20](#)
- modifying MAC address table multiport unicast entry, [20](#)
- performing interface loopback test (Ethernet), [4](#)
- performing LAN switching spanning tree mCheck, [88](#)
- performing LAN switching spanning tree mCheck globally, [88](#)
- performing LAN switching spanning tree mCheck in interface view, [89](#)
- restoring Ethernet link aggregate interface default settings, [45](#)
- setting Ethernet link aggregate group Selected ports min/max, [43](#)
- setting Ethernet link aggregate interface (expected bandwidth), [44](#)
- setting Ethernet link aggregation load sharing mode (global), [46](#)
- setting Ethernet link aggregation load sharing mode (group-specific), [46](#)
- setting interface MDIX mode (Layer 2 Ethernet), [10](#)
- setting interface statistics polling interval (Ethernet), [6](#)
- setting L2PT tunneled packet destination multicast MAC address, [110](#)
- setting LAN switching LLDP frame encapsulation format, [239](#)
- setting LAN switching LLDP operating mode, [235](#)
- setting LAN switching LLDP parameters, [239](#)
- setting LAN switching LLDP reinitialization delay, [236](#)
- setting LAN switching spanning tree mode, [74](#)
- setting loop detection interval, [119](#)
- setting QinQ SVLAN tag 802.1p priority, [202](#)
- shutting down Ethernet link aggregate interface, [45](#)

- specifying LAN switching spanning tree port path cost calculation standard, [82](#)
- specifying Layer 2 aggregate interface (ignored VLAN), [43](#)
- testing interface cable connection (Layer 2 Ethernet), [10](#)

protecting

- LAN switching spanning tree protection functions, [94](#)
- spanning tree SNMP notification (new-root election, topology change events), [98](#)

protocol-based VLAN

- configuration, [135](#), [142](#)

protocols and standards

- Ethernet link aggregation protocol configuration, [35](#)
- LAN switching LLDP, [234](#)
- LAN switching MSTP, [71](#)
- LAN switching STP protocol packets, [58](#)
- MVRP, [185](#)
- QinQ, [199](#)
- VLAN, [124](#)

PVID (port-based VLAN), [126](#)

PVST, [58](#), *See also* [STP](#)

- configuration, [73](#), [103](#)
- feature enable, [88](#)
- mode set, [74](#)
- port links, [66](#)

Q

QinQ

- basic QinQ configuration, [204](#)
- configuration, [198](#), [204](#)
- configuration restrictions, [200](#)
- CVLAN tag, [198](#)
- CVLAN tag TPID value, [202](#)
- displaying, [203](#)
- enable, [200](#)
- how it works, [198](#)
- implementation, [199](#)
- loop detection configuration, [116](#), [118](#), [120](#)
- protocols and standards, [199](#)
- SVLAN tag, [198](#)
- SVLAN tag 802.1p priority, [202](#)
- SVLAN tag TPID value, [202](#)
- VLAN tag TPID value, [201](#)
- VLAN transparent transmission, [200](#)
- VLAN transparent transmission configuration, [206](#)

QoS

- QinQ SVLAN tag 802.1p priority, [202](#)

- voice VLAN interface QoS priority settings configuration, [173](#)

queuing

- MAC Information queue length, [31](#)

R

Rapid Spanning Tree Protocol. *Use* [RSTP](#)

rate

- LAN switching spanning tree BPDU transmission rate, [80](#)

receiving

- LAN switching LLDP frames, [233](#)

recovering

- loop detection port status auto recovery, [117](#)

redirecting

- Ethernet link aggregation traffic redirection, [47](#)

reference port (Ethernet link aggregation), [36](#), [38](#)

region

- LAN switching MST, [67](#)
- LAN switching MST region configuration, [75](#)
- LAN switching MST region max hops, [78](#)
- LAN switching MST regional root, [68](#)

registering

- MVRP registration fixed mode, [184](#)
- MVRP registration forbidden mode, [184](#)
- MVRP registration mode, [186](#)
- MVRP registration normal mode, [184](#)

reinitialization delay (LLDP), [236](#)

restoring

- Ethernet link aggregate interface default settings, [45](#)

restrictions

- bulk interface configuration, [15](#)
- Ethernet link aggregation group, [41](#)
- Ethernet link aggregation traffic redirection, [47](#)
- fiber ports forcibly bringing up, [9](#)
- LAN switching spanning tree mode configuration, [75](#)
- LAN switching spanning tree port role restriction, [96](#)
- LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
- LAN switching STP Digest Snooping configuration, [89](#)
- LAN switching STP edge port configuration, [81](#)
- LAN switching STP mCheck configuration, [88](#)
- LAN switching STP port link type configuration, [85](#)
- LAN switching STP TC Snooping configuration, [94](#)
- LAN switching STP timer configuration, [79](#)
- loopback testing (Ethernet), [4](#)
- MVRP configuration, [185](#)

- QinQ configuration, [200](#)
- root
 - LAN switching MST common root bridge, [68](#)
 - LAN switching MST regional root, [68](#)
 - LAN switching MST root port role, [69](#)
 - LAN switching spanning tree root bridge, [76](#)
 - LAN switching spanning tree root bridge (device), [77](#)
 - LAN switching spanning tree root guard, [95](#)
 - LAN switching spanning tree secondary root bridge (device), [77](#)
 - LAN switching STP algorithm calculation, [60](#)
 - LAN switching STP root bridge, [59](#)
 - LAN switching STP root port, [59](#)
- routing
 - configuring MAC-based VLAN dynamic assignment, [133](#)
 - configuring MAC-based VLAN static assignment, [132](#)
 - configuring server-assigned MAC-based VLAN, [133](#)
 - connecting host and IP phone in series, [170](#)
 - connecting IP phone to device, [170](#)
 - IP subnet-based VLAN configuration, [134](#), [141](#)
 - MAC-based VLAN configuration, [129](#), [139](#)
 - MAC-based VLAN dynamic assignment, [130](#)
 - MAC-based VLAN static assignment, [129](#)
 - protocol-based VLAN configuration, [135](#), [142](#)
 - server-assigned MAC-based VLAN, [131](#)
 - voice VLAN automatic assignment mode port operation configuration, [174](#), [178](#)
 - voice VLAN configuration, [168](#), [178](#)
 - voice VLAN interface QoS priority settings configuration, [173](#)
 - voice VLAN IP phone access method, [170](#)
 - voice VLAN manual assignment mode port operation configuration, [175](#), [180](#)
- RSTP, [58](#), *See also* STP
 - configuration, [72](#)
 - feature enable, [87](#)
 - mode set, [74](#)
 - MSTP device implementation, [71](#)
 - network convergence, [65](#)
- rule
 - MAC address table unknown frame forwarding rule, [23](#)
- S**
- security
 - voice VLAN mode, [172](#)
- selecting
 - Ethernet link aggregation Selected ports min/max, [43](#)
 - Ethernet link aggregation selected state, [34](#)
 - Ethernet link aggregation unselected state, [34](#)
- server-assigned
 - configuring MAC-based VLAN, [133](#)
 - MAC-based VLAN, [131](#)
- service
 - LAN switching LLDP service bridge mode, [235](#)
- setting
 - Ethernet link aggregate group Selected ports min/max, [43](#)
 - Ethernet link aggregate interface (expected bandwidth), [44](#)
 - Ethernet link aggregation load sharing mode (global), [46](#)
 - Ethernet link aggregation load sharing mode (group-specific), [46](#)
 - Ethernet link aggregation member port state, [36](#), [39](#)
 - interface MDIX mode (Layer 2 Ethernet), [10](#)
 - interface statistics polling interval (Ethernet), [6](#)
 - L2PT tunneled packet destination multicast MAC address, [110](#)
 - LAN switching LLDP frame encapsulation format, [239](#)
 - LAN switching LLDP operating mode, [235](#)
 - LAN switching LLDP parameters, [239](#)
 - LAN switching LLDP reinitialization delay, [236](#)
 - LAN switching spanning tree mode, [74](#)
 - loop detection interval, [119](#)
 - QinQ SVLAN tag 802.1p priority, [202](#)
- shutting down
 - Ethernet link aggregate interface, [45](#)
 - loop detection shutdown action, [117](#)
- SNAP
 - LAN switching LLDP frame encapsulated in SNAP format, [228](#)
 - LAN switching LLDP frame encapsulation format, [239](#)
- SNMP
 - MAC Information configuration, [30](#), [31](#)
- snooping
 - LAN switching spanning tree Digest Snooping, [89](#), [90](#)
 - LAN switching spanning tree TC Snooping, [93](#)
- spanning tree, [58](#), *See also* STP, RSTP, PVST, MSTP
 - BPDU drop, [98](#)
 - BPDU guard enable, [95](#)
 - BPDU transmission rate configuration, [80](#)
 - configuration, [58](#), [71](#), [100](#)
 - device priority configuration, [77](#)

- Digest Snooping, 89, 90
- displaying, 99
- edge port configuration, 81
- feature enable, 87
- loop guard enable, 96
- maintaining, 99
- mCheck, 88
- mode configuration restrictions, 75
- mode set, 74
- MST region max hops, 78
- MSTP, 66, *See also* MSTP
- No Agreement Check, 91, 93
- port link type configuration, 85
- port mode configuration, 86
- port path cost calculation standard, 82
- port path cost configuration, 81, 84
- port priority configuration, 85
- port role restriction, 96
- port state transition output, 87
- protection functions, 94
- PVST, 66, *See also* PVST
- root bridge configuration, 76
- root bridge configuration (device), 77
- root guard enable, 95
- RSTP, 65, *See also* RSTP
- secondary root bridge configuration (device), 77
- SNMP notification enable (new-root election, topology change events), 98
- switched network diameter, 78
- TC Snooping, 93
- TC-BPDU guard, 97
- TC-BPDU transmission restriction, 97
- timeout factor configuration, 80
- timer configuration, 79
- specifying
 - LAN switching spanning tree port path cost calculation standard, 82
 - Layer 2 aggregate interface (ignored VLAN), 43
- state
 - Ethernet link aggregation member port state, 34, 36, 39
 - interface state change suppression (Ethernet), 3
- static
 - configuring MAC-based VLAN static assignment, 132
 - Ethernet link aggregation (Layer 2), 48
 - Ethernet link aggregation (static mode), 36
 - Ethernet link aggregation group, 41
 - Ethernet link aggregation group BFD, 44
 - Ethernet link aggregation mode, 35
 - Layer 2 Ethernet link aggregation group, 41
 - MAC address table entry, 17
 - MAC-based VLAN static assignment, 129
 - static MAC address entry
 - static source check disable, 27
 - statistics
 - interface statistics polling interval (Ethernet), 6
 - storm
 - interface storm control (Layer 2 Ethernet), 7
 - interface storm suppression (Layer 2 Ethernet), 6
 - STP
 - algorithm calculation, 60
 - basic concepts, 59
 - BPDU forwarding, 64
 - configuration, 72
 - designated bridge, 59
 - designated port, 59
 - Digest Snooping configuration restrictions, 89
 - edge port configuration restrictions, 81
 - feature enable, 87
 - L2PT for STP configuration, 111
 - loop detection, 58
 - mCheck configuration restrictions, 88
 - mode set, 74
 - MSTP device implementation, 71
 - path cost, 60
 - port link type configuration restrictions, 85
 - protocol packets, 58
 - root bridge, 59
 - root port, 59
 - TC Snooping configuration restrictions, 94
 - timer configuration restrictions, 79
 - timers, 65
 - sub VLAN
 - configuration, 146
 - subnetting
 - IP subnet-based VLAN configuration, 134, 141
 - super VLAN
 - configuration, 146, 146, 148
 - displaying, 147
 - interface configuration, 147
 - sub VLAN creation, 146
 - suppressing
 - interface physical state change suppression (Ethernet), 3
 - interface storm control configuration (Layer 2 Ethernet), 7
 - interface storm suppression (Layer 2 Ethernet), 6
 - SVLAN

- basic QinQ configuration, [204](#)
- QinQ configuration, [198](#), [204](#)
- QinQ SVLAN tag 802.1p priority, [202](#)
- QinQ VLAN transparent transmission configuration, [206](#)
- VLAN mapping configuration, [208](#), [213](#), [220](#)
- VLAN mapping implementation, [210](#)
- switching
 - inloopback interface configuration, [13](#), [14](#)
 - interface configuration (Ethernet), [1](#)
 - LAN switching spanning tree switched network diameter, [78](#)
 - loopback interface configuration, [13](#), [13](#)
 - MAC address table configuration, [17](#), [18](#), [28](#)
 - null interface configuration, [13](#), [13](#)
- synchronizing
 - MAC addresses, [24](#)
- system
 - interface bulk configuration, [15](#)
- T**
- table
 - LAN switching MSTP VLAN-to-instance mapping table, [68](#)
 - MAC address, [17](#), [18](#), [28](#)
- tag
 - QinQ CVLAN tag, [198](#)
 - QinQ CVLAN tag TPID value, [202](#)
 - QinQ SVLAN tag, [198](#)
 - QinQ SVLAN tag 802.1p priority, [202](#)
 - QinQ SVLAN tag TPID value, [202](#)
 - QinQ VLAN tag TPID value, [201](#)
 - VLAN mapping configuration, [208](#), [213](#), [220](#)
 - VLAN mapping configuration (1\1), [214](#), [220](#)
 - VLAN mapping configuration (1\2), [218](#), [224](#)
 - VLAN mapping configuration (2\2), [219](#), [224](#)
 - VLAN mapping configuration (M1), [214](#), [220](#)
 - VLAN mapping configuration (M1) (dynamic IP address assignment), [215](#)
 - VLAN mapping configuration (M1) (static IP address assignment), [217](#)
- TC Snooping (spanning tree), [93](#)
- TC-BPDU
 - LAN switching spanning tree TC-BPDU guard, [97](#)
 - LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
- testing
 - interface cable connection (Layer 2 Ethernet), [10](#)
- time
 - Ethernet link aggregation LACP timeout interval, [37](#)
- timeout
 - Ethernet link aggregation LACP long timeout interval, [38](#)
 - Ethernet link aggregation LACP short timeout interval, [38](#)
 - LAN switching spanning tree timeout factor, [80](#)
- timer
 - LAN switching LLDP reinitialization delay, [236](#)
 - LAN switching spanning tree forward delay, [79](#)
 - LAN switching spanning tree hello, [79](#)
 - LAN switching spanning tree max age, [79](#)
 - LAN switching STP forward delay, [65](#)
 - LAN switching STP hello, [65](#)
 - LAN switching STP max age, [65](#)
 - MAC address table dynamic aging timer, [22](#)
 - MRP Join, [184](#)
 - MRP Leave, [184](#)
 - MRP LeaveAll, [184](#)
 - MRP Periodic, [184](#)
 - MVRP configuration, [187](#)
- TLV
 - LAN switching LLDP advertisable TLV configuration, [237](#)
 - LAN switching LLDP management address configuration, [238](#)
 - LAN switching LLDP management address encoding format, [238](#)
 - LAN switching LLDP parameters, [239](#)
 - LAN switching LLDPDU basic management types, [230](#)
 - LAN switching LLDPDU LLDP-MED types, [230](#)
 - LAN switching LLDPDU management address TLV, [233](#)
 - LAN switching LLDPDU organization-specific types, [230](#)
- topology
 - LAN switching STP TCN BPDU protocol packets, [58](#)
- traffic
 - Ethernet link aggregation traffic redirection, [47](#)
- transmitting
 - LAN switching LLDP frames, [233](#)
 - LAN switching spanning tree TC-BPDU transmission restriction, [97](#)
 - QinQ VLAN transparent transmission, [200](#), [206](#)
- transparent transmission (QinQ for VLAN), [200](#), [206](#)
- trapping
 - LAN switching LLDP configuration, [242](#)
 - LAN switching LLDP-MED configuration, [242](#)
 - MAC Information configuration, [30](#), [31](#)

- MAC Information mode configuration, 30
- trunk port
 - port-based VLAN assignment (trunk port), 128
- tunneling
 - L2PT configuration, 107, 109, 111
 - L2PT enable, 109
 - L2PT for LACP configuration, 112
 - L2PT for STP configuration, 111
 - L2PT tunneled packet destination multicast MAC address, 110

U

- unicast
 - MAC address table configuration, 17, 18, 28
 - MAC address table multiport unicast entry, 17

V

Virtual Local Area Network. *Use* [VLAN](#)

VLAN

- aggregation, 146. *See also* [super VLAN](#)
- basic configuration, 124
- basic QinQ configuration, 204
- configuration, 123, 137
- configuring MAC-based static assignment, 132
- configuring server-assigned MAC-based, 133
- displaying, 137
- frame encapsulation, 123
- group configuration, 136
- interface basics configuration, 125
- IP subnet-based configuration, 134, 141
- L2PT configuration, 107, 109, 111
- L2PT for LACP configuration, 112
- L2PT for STP configuration, 111
- LAN switching LLDP CDP compatibility, 240
- LAN switching LLDP configuration (CDP-compatible), 247
- LAN switching MSTP VLAN-to-instance mapping table, 68
- LAN switching PVST, 66
- Layer 2 Ethernet aggregate interface (ignored VLAN), 43
- Layer 2 LAN switching port isolation configuration, 55
- loop detection configuration, 116, 118, 120
- MAC-based configuration, 129, 139
- MAC-based dynamic assignment, 130
- MAC-based static assignment, 129
- maintaining, 137
- mapping. *See* [VLAN mapping](#)
- MRP implementation, 182
- MVRP configuration, 182, 185, 188

- MVRP GVRP compatibility, 187
- port link type, 126
- port-based configuration, 126, 137
- port-based VLAN assignment (access port), 127
- port-based VLAN assignment (hybrid port), 128
- port-based VLAN assignment (trunk port), 128
- port-based VLAN frame handling, 126
- private VLAN configuration, 151, 152
- protocol-based configuration, 135, 142
- protocols and standards, 124
- PVID, 126
- QinQ configuration, 198, 204
- QinQ CVLAN tag, 198
- QinQ CVLAN tag TPID value, 202
- QinQ implementation, 199
- QinQ SVLAN tag, 198
- QinQ SVLAN tag 802.1p priority, 202
- QinQ SVLAN tag TPID value, 202
- QinQ transparent transmission, 200
- QinQ VLAN tag TPID value, 201
- QinQ VLAN transparent transmission configuration, 206
- server-assigned MAC-based, 131
- super VLAN configuration, 146, 146, 148
- super VLAN interface configuration, 147
- termination. *See* [VLAN termination](#)
- voice VLAN assignment mode, 170, 170
- voice VLAN automatic assignment mode port operation configuration, 174, 178
- voice VLAN configuration, 168, 178
- voice VLAN interface QoS priority settings configuration, 173
- voice VLAN IP phone access method, 170
- voice VLAN manual assignment mode port operation configuration, 175, 180
- voice VLAN security mode, 172

VLAN mapping

- 1\1 application scenario, 208
- 1\1 configuration, 214, 220
- 1\1 implementation, 210, 211
- 1\2 application scenario, 210
- 1\2 configuration, 218, 224
- 1\2 implementation, 210, 212
- 2\2 application scenario, 210
- 2\2 configuration, 219, 224
- 2\2 implementation, 210, 212
- ARP detection (M\1) (dynamic IP address assignment), 215
- ARP snooping (M\1) (static IP address assignment), 217
- configuration, 208, 213, 220

- DHCP snooping (M\1) (dynamic IP address assignment), [215](#)
- displaying, [220](#)
- M\1 application scenario, [208](#)
- M\1 configuration, [214](#), [220](#)
- M\1 configuration (dynamic IP address assignment), [215](#)
- M\1 configuration (static IP address assignment), [217](#)
- M\1 customer-side port (dynamic IP address assignment), [216](#)
- M\1 customer-side port (static IP address assignment), [217](#)
- M\1 implementation, [210](#), [211](#)
- M\1 network-side port (dynamic IP address assignment), [216](#)
- M\1 network-side port (static IP address assignment), [218](#)
- voice traffic
 - LAN switching LLDP CDP compatibility, [240](#)
 - LAN switching LLDP configuration (CDP-compatible), [247](#)
- voice VLAN
 - advertising authorization VLANs through LLDP/CDP dynamically, [177](#)
 - advertising voice VLAN information to IP phones, [169](#)
 - assignment mode, [170](#)
 - automatic assignment mode, [170](#)
 - automatic assignment mode port operation configuration, [174](#), [178](#)
 - automatically identifying IP phones through LLDP, [169](#)
 - configuration, [168](#), [178](#)
 - configuring LLDP/CDP to advertise a voice VLAN, [176](#)
 - configuring voice VLAN on a port, [170](#)
 - connecting host and IP phone in series, [170](#)
 - connecting IP phone to device, [170](#)
 - cooperation of voice VLAN assignment modes and IP phones, [171](#)
 - displaying, [177](#)
 - enabling LLDP for automatic IP phone discovery, [175](#)
 - identifying IP phones through OUI address, [168](#)
 - interface QoS priority settings configuration, [173](#)
 - IP phone access method, [170](#)
 - manual assignment mode, [171](#)
 - manual assignment mode port operation configuration, [175](#), [180](#)
 - methods of identifying IP phones, [168](#)
 - normal mode, [172](#)
 - security mode, [172](#)
- VoIP
 - voice VLAN IP phone access method, [170](#)
- VPN
 - basic QinQ configuration, [204](#)
 - QinQ configuration, [198](#), [204](#)
 - QinQ VLAN transparent transmission configuration, [206](#)