HPE FlexFabric 5940 & 5930 Switch Series
Layer 2—LAN Switching Configuration Guide
Setting load sharing modes for link aggregation groups ........................................... 69
Specifying ignored packet fields for default link-aggregation load sharing ................ 70
Enabling local-first load sharing for link aggregation .................................................. 71
Configuring link aggregation load sharing algorithm settings .................................... 72
Setting the global load sharing mode for MAC-in-MAC traffic .................................. 72
Enabling link-aggregation traffic redirection ............................................................. 72
About link-aggregation traffic redirection ................................................................. 72
Configuration restrictions and guidelines ................................................................. 73
Enabling link-aggregation traffic globally ............................................................... 73
Enabling link-aggregation traffic redirection for an aggregation group ..................... 73
Specifying link aggregation management VLANs and management port .................. 74
Excluding a subnet from load sharing on aggregate links ......................................... 74
Enabling a Layer 2 aggregate interface to reflect incoming packets back ................... 75
Enabling transparent LACPDU transmission ......................................................... 76
Configuring S-MLAG ............................................................................................... 77
Displaying and maintaining Ethernet link aggregation .............................................. 78
Ethernet link aggregation configuration examples .................................................... 79
Layer 2 static aggregation configuration example ..................................................... 79
Layer 2 dynamic aggregation configuration example ................................................ 80
Layer 2 aggregation load sharing configuration example .......................................... 82
Layer 2 edge aggregate interface configuration example ......................................... 85
Layer 3 static aggregation configuration example .................................................... 86
Layer 3 dynamic aggregation configuration example ................................................ 87
Layer 3 aggregation load sharing configuration example .......................................... 89
S-MLAG configuration example ............................................................................... 91

Configuring port isolation ......................................................................................... 94
Assigning a port to an isolation group ....................................................................... 94
Displaying and maintaining port isolation ............................................................... 94
Port isolation configuration example ....................................................................... 95
Network requirements ............................................................................................... 95
Configuration procedure ......................................................................................... 95
Verifying the configuration ....................................................................................... 95

Configuring spanning tree protocols ........................................................................ 97
STP ......................................................................................................................... 97
STP protocol frames ............................................................................................... 97
Basic concepts in STP .............................................................................................. 99
Calculation process of the STP algorithm ................................................................ 100
RSTP ..................................................................................................................... 106
RSTP protocol frames ............................................................................................ 106
Basic concepts in RSTP ......................................................................................... 106
How RSTP works ................................................................................................. 107
RSTP BPDU processing .......................................................................................... 107
PVST ...................................................................................................................... 108
PVST protocol frames ............................................................................................ 108
Basic concepts in PVST ........................................................................................ 109
How PVST works .................................................................................................. 109
MSTP ...................................................................................................................... 109
MSTP features ....................................................................................................... 109
MSTP protocol frames ............................................................................................ 109
MSTP basic concepts ............................................................................................. 111
How MSTP works ................................................................................................ 114
MSTP implementation on devices .......................................................................... 115
Rapid transition mechanism .................................................................................. 115
Protocols and standards ......................................................................................... 117
Spanning tree configuration task lists ...................................................................... 118
STP configuration task list .................................................................................... 118
RSTP configuration task list ................................................................................... 119
PVST configuration task list .................................................................................. 120
MSTP configuration task list .................................................................................. 121
Setting the spanning tree mode ............................................................................. 121
Configuring an MST region ............................................................................................................ 122
Configuring the root bridge or a secondary root bridge ................................................................. 123
  Configuring the device as the root bridge of a specific spanning tree ............................................ 123
  Configuring the device as a secondary root bridge of a specific spanning tree ......................... 124
Configuring the device priority ...................................................................................................... 124
Configuring the maximum hops of an MST region ......................................................................... 124
Configuring the network diameter of a switched network ............................................................. 125
Setting spanning tree timers ......................................................................................................... 125
  Configuration restrictions and guidelines ..................................................................................... 126
  Configuration procedure ............................................................................................................. 126
Setting the timeout factor .............................................................................................................. 127
Configuring the BPDU transmission rate ....................................................................................... 127
Configuring edge ports .................................................................................................................. 128
  Configuration restrictions and guidelines ..................................................................................... 128
  Configuration procedure ............................................................................................................. 128
Configuring path costs of ports ...................................................................................................... 128
  Specifying a standard for the device to use when it calculates the default path cost .................. 128
  Configuring path costs of ports .................................................................................................... 131
  Configuration example ................................................................................................................ 131
Configuring the port priority .......................................................................................................... 132
Configuring the port link type ........................................................................................................ 132
  Configuration restrictions and guidelines ..................................................................................... 132
  Configuration procedure ............................................................................................................. 132
Configuring the mode a port uses to recognize and send MSTP frames ..................................... 133
Enabling outputting port state transition information .................................................................... 133
Enabling the spanning tree feature ............................................................................................... 134
  Enabling the spanning tree feature in STP/RSTP/MSTP mode .................................................... 134
  Enabling the spanning tree feature in PVST mode ...................................................................... 134
Performing mCheck ..................................................................................................................... 135
  Configuration restrictions and guidelines ..................................................................................... 135
  Performing mCheck globally ........................................................................................................ 135
  Performing mCheck in interface view ........................................................................................ 136
Disabling inconsistent PVID protection ......................................................................................... 136
Configuring Digest Snooping ......................................................................................................... 136
  Configuration restrictions and guidelines ..................................................................................... 137
  Configuration procedure ............................................................................................................. 137
  Digest Snooping configuration example ....................................................................................... 137
Configuring No Agreement Check ............................................................................................... 138
  Configuration prerequisites .......................................................................................................... 139
  Configuration procedure ............................................................................................................. 140
  No Agreement Check configuration example ............................................................................. 140
Configuring TC Snooping .............................................................................................................. 140
  Configuration restrictions and guidelines ..................................................................................... 141
  Configuration procedure ............................................................................................................. 141
Configuring protection features .................................................................................................... 142
  Configuring BPDU guard .............................................................................................................. 142
  Enabling root guard .................................................................................................................... 143
  Enabling loop guard .................................................................................................................... 143
  Configuring port role restriction ................................................................................................. 144
  Configuring TC-BPDU transmission restriction .......................................................................... 144
  Enabling TC-BPDU guard ............................................................................................................ 145
  Enabling BPDU drop .................................................................................................................... 145
  Enabling PVST BPDU guard ........................................................................................................ 146
  Disabling dispute guard .............................................................................................................. 146
Enabling the device to log events of detecting or receiving TC BPDUs ...................................... 148
Disabling the device to reactivate the shutdown edge ports ............................................................ 148
Enabling BPDU transparent transmission on a port ....................................................................... 148
Enabling SNMP notifications for new-root election and topology change events .................... 149
Displaying and maintaining the spanning tree ............................................................................ 149
Spanning tree configuration examples .......................................................................................... 150
  MSTP configuration example ...................................................................................................... 150
  PVST configuration example ...................................................................................................... 154
Configuring super VLANs .......................................................... 192

Super VLAN configuration task list ........................................ 192
Creating a sub-VLAN ............................................................... 192
Configuring a super VLAN ..................................................... 192
Configuring a super VLAN interface ....................................... 193
Displaying and maintaining super VLANs ............................. 193
Super VLAN configuration example ....................................... 194
Network requirements ........................................................... 194
Configuration procedure ....................................................... 194
Verifying the configuration ..................................................... 195
Configuring Ethernet interfaces

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

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

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 or virtual slot number of the PEX on an IRF 3.1 system. If the switch is not in an IRF fabric, A is 1 by default.
- **B**—Card slot number. 0 indicates the interface is a fixed interface of the switch. 1 indicates the interface is on expansion interface-card 1. 2 indicates the interface is on expansion interface-card 2.
- **C**—Port index.

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

Configuring a management Ethernet interface

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

In an IRF system, each member device has physical management Ethernet interfaces. To back up a management link, use a cable to connect two management Ethernet interfaces of the same number on the master device and a subordinate device. The two management Ethernet interfaces back up each other as follows:

- When the management Ethernet interface on the master device is in normal state, it is the only one that processes management traffic.
- When the management Ethernet interface on the master device fails, the management Ethernet interface on the subordinate device takes over to process management traffic.
- When the management Ethernet interface on the master device recovers, it takes over to process management traffic again.

To configure a management Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter management Ethernet interface view.</td>
<td>interface M-GigabitEthernet interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Set the interface description.</td>
<td>description text</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Shut down</td>
<td>shutdown</td>
</tr>
</tbody>
</table>
Configuring common Ethernet interface settings

This section describes the settings common to Layer 2 Ethernet interfaces, Layer 3 Ethernet interfaces, and Layer 3 Ethernet subinterfaces. For more information about the settings specific to Layer 2 Ethernet interfaces or subinterfaces, see "Configuring a Layer 2 Ethernet interface." For more information about the settings specific to Layer 3 Ethernet interfaces or subinterfaces, see "Configuring a Layer 3 Ethernet interface or subinterface."

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

The following 40-GE interfaces cannot be split into 10-GE breakout interfaces:

- 40-GE interfaces FortyGigE 1/0/1 through FortyGigE 1/0/4 and FortyGigE 1/0/29 through FortyGigE 1/0/32 on the following switches:
  - HPE FlexFabric 5930-32QSFP+ Switch (JG726A).
  - HPE FlexFabric 5930-32QSFP+ TAA Switch (JG727A).
  - HPE FlexFabric 5940 32QSFP+ Switch (JH396A).

- 100-GE interfaces on the following switches:
  - HPE FlexFabric 5940 48SFP+ 6QSFP28 Switch (JH390A).
  - HPE FlexFabric 5940 48XGT 6QSFP28 Switch (JH391A).

- The last two interfaces on an LSWM18QC (JH183A) or LSWM18CQMSEC (JH957A) interface card of the following switches:
  - HPE FlexFabric 5940 4-slot Switch (JH398A).
  - HPE FlexFabric 5930-4Slot Switch (JH179A).
  - HPE FlexFabric 5930-4Slot TAA Switch (JH188A).

The LSWM18CQMSEC (JH957A) interface card is supported only in Release 2612 and later versions. Interfaces on the LSWM18CQMSEC card do not support QSFP28 transceiver modules or cables and support only QSFP+ transceiver modules and cables when the card is installed in the following switches:

- HPE FlexFabric 5930-2Slot+2QSFP+ Switch (JH178A).
- HPE FlexFabric 5930-2Slot+2QSFP+ TAA Switch (JH187A).
- HPE FlexFabric 5940 2-slot Switch (JH397A).
- HPE FlexFabric 5930-4Slot Switch.
- HPE FlexFabric 5930-4Slot TAA Switch.
- HPE FlexFabric 5940 4-slot Switch.

- 40-GE interfaces on an LSWM124XGT2Q (JH182A), LSWM124XG2Q (JH181A), LSWM124XG2QL (JH180A), or LSWM124XG2QFC (JH184A) interface card of the following switches:
  - HPE FlexFabric 5940 4-slot Switch.
  - HPE FlexFabric 5930-4Slot Switch.
  - HPE FlexFabric 5930-4Slot TAA Switch.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>the interface.</td>
<td>interface is up.</td>
<td></td>
</tr>
</tbody>
</table>
Splitting a 40-GE interface into four 10-GE breakout interfaces

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

For example, you can split 40-GE interface FortyGigE 1/0/1 into four 10-GE breakout interfaces Ten-GigabitEthernet 1/0/1:1 through Ten-GigabitEthernet 1/0/1:4.

After you configure this feature on a 40-GE interface, the system deletes the 40-GE interface and creates the four 10-GE breakout interfaces.

After the `using tengige` command is successfully configured, you do not need to reboot the switch. You can view the four 10-GE breakout interfaces by using the `display interface brief` command.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>using tengige</td>
<td>By default, a 40-GE interface is not split and operates as a single interface. The 10-GE breakout interfaces support the same configuration and attributes as common 10-GE interfaces, except that they are numbered differently.</td>
</tr>
</tbody>
</table>

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

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

After you configure this feature on a 10-GE breakout interface, the system deletes the four 10-GE breakout interfaces and creates the 40-GE interface.

After the `using fortygige` command is successfully configured, you do not need to reboot the switch. You can view the 40-GE interface by using the `display interface brief` command.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>using fortygige</td>
<td>By default, a 10-GE breakout interface operates as a single interface.</td>
</tr>
</tbody>
</table>
Configuring basic settings of an Ethernet interface or subinterface

You can configure an Ethernet interface to operate in one of the following duplex modes:

- **Full-duplex mode**—The interface can send and receive packets simultaneously.
- **Half-duplex mode**—The interface can only send or receive packets at a given time.
- **Autonegotiation mode**—The interface negotiates a duplex mode with its peer.

You can set the speed of an Ethernet interface or enable it to automatically negotiate a speed with its peer.

### Configuring an Ethernet interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td><strong>interface interface-type interface-number</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Set the description for the Ethernet interface.</td>
<td><strong>description text</strong></td>
</tr>
<tr>
<td>4.</td>
<td>Set the duplex mode for the Ethernet interface.</td>
<td>**duplex { auto</td>
</tr>
<tr>
<td>5.</td>
<td>Set the speed for the Ethernet interface.</td>
<td>**speed { 10</td>
</tr>
<tr>
<td>6.</td>
<td>Set the expected bandwidth for the Ethernet interface.</td>
<td><strong>bandwidth bandwidth-value</strong></td>
</tr>
<tr>
<td>7.</td>
<td>Restore the default settings for the Ethernet interface.</td>
<td><strong>default</strong></td>
</tr>
<tr>
<td>8.</td>
<td>Bring up the Ethernet interface.</td>
<td><strong>undo shutdown</strong></td>
</tr>
</tbody>
</table>

### Configuring an Ethernet subinterface

To associate a VPN instance with a Layer 3 Ethernet subinterface, make sure one or more of the following conditions are met:

- A Layer 3 aggregate subinterface and a VLAN interface that have the same number as the Layer 3 Ethernet subinterface are associated with the VPN instance.
- Packet statistics is enabled on the Layer 3 Ethernet subinterface.
For more information about Layer 3 aggregate subinterfaces, see Ethernet link aggregation in *Layer 2—LAN Switching Configuration Guide*. For more information about VLAN interfaces, see VLAN in *Layer 2—LAN Switching Configuration Guide*. For more information about associating a VPN instance with an interface, see MPLS L3VPN and MCE in *MPLS Configuration Guide*.

To configure an Ethernet subinterface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an Ethernet subinterface.</td>
<td>interface interface-type interface-number.subnumber</td>
</tr>
<tr>
<td>3.</td>
<td>Set the description for the Ethernet subinterface.</td>
<td>description text</td>
</tr>
<tr>
<td>4.</td>
<td>Restore the default settings for the Ethernet subinterface.</td>
<td>default</td>
</tr>
<tr>
<td>5.</td>
<td>Set the expected bandwidth for the Ethernet subinterface.</td>
<td>bandwidth bandwidth-value</td>
</tr>
<tr>
<td>6.</td>
<td>Bring up the Ethernet subinterface.</td>
<td>undo shutdown</td>
</tr>
</tbody>
</table>

### Configuring the link mode of an Ethernet interface

**CAUTION:**

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

The interfaces on this Switch Series can operate either as Layer 2 or Layer 3 Ethernet interfaces. You can set the link mode to bridge or route.

To configure the link mode of an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the link mode of the Ethernet interface.</td>
<td>port link-mode ( bridge</td>
</tr>
</tbody>
</table>
Configuring jumbo frame support

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

The Ethernet interface processes jumbo frames in the following ways:

- When the Ethernet interface is configured to deny jumbo frames, the Ethernet interface discards jumbo frames.
- When the Ethernet interface is configured with jumbo frame support, the Ethernet interface performs the following operations:
  - Processes jumbo frames within the specified length.
  - Discards jumbo frames that exceed the specified length.

To configure jumbo frame support in interface view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure jumbo frame support.</td>
<td>jumboframe enable [ size ]</td>
</tr>
</tbody>
</table>

By default, the switch allows jumbo frames within 10000 bytes to pass through all Ethernet interfaces.

Configuring physical state change suppression on an Ethernet interface

**IMPORTANT:**

Do not enable this feature on an interface that has RRPP, 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 an interface comes up or goes down, the interface immediately reports the change to the CPU. The CPU then performs the following operations:

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

To prevent frequent physical link flapping from affecting system performance, configure physical state change suppression. You can configure this feature to suppress only link-down events, only link-up events, or both. If an event of the specified type still exists when the suppression interval expires, the system reports the event.

When you configure this feature, follow these guidelines:

- To suppress only link-down events, configure the `link-delay [ msec ] delay-time` command.
- To suppress only link-up events, configure the `link-delay [ msec ] delay-time mode up` command.
- To suppress both link-down and link-up events, configure the `link-delay [ msec ] delay-time mode updown` command.
- The `link-delay`, `dampening`, and `port link-flap protect enable` commands are mutually exclusive on an Ethernet interface.
To configure physical state change suppression on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure physical state change suppression.</td>
<td>link-delay [ msec ] delay-time [ mode { up</td>
</tr>
</tbody>
</table>

### Configuring dampening on an Ethernet interface

The interface dampening feature uses an exponential decay mechanism to prevent excessive interface flapping events from adversely affecting routing protocols and routing tables in the network. Suppressing interface state change events protects the system resources.

If an interface is not dampened, its state changes are reported. For each state change, the system also generates an SNMP trap and log message.

After a flapping interface is dampened, it does not report its state changes to the CPU. For state change events, the interface only generates SNMP traps and log messages.

#### Parameters

- **Penalty**—The interface has an initial penalty of 0. When the interface flaps, the penalty increases by 1000 for each down event until the ceiling is reached. It does not increase for up events. When the interface stops flapping, the penalty decreases by half each time the half-life timer expires until the penalty drops to the reuse threshold.

- **Ceiling**—The penalty stops increasing when it reaches the ceiling.

- **Suppress-limit**—The accumulated penalty that triggers the device to dampen the interface. In dampened state, the interface does not report its state changes to the CPU. For state change events, the interface only generates SNMP traps and log messages.

- **Reuse-limit**—When the accumulated penalty decreases to this reuse threshold, the interface is not dampened. Interface state changes are reported to the upper layers. For each state change, the system also generates an SNMP trap and log message.

- **Decay**—The amount of time (in seconds) after which a penalty is decreased.

- **Max-suppress-time**—The maximum amount of time the interface can be dampened. If the penalty is still higher than the reuse threshold when this timer expires, the penalty stops increasing for down events. The penalty starts to decrease until it drops below the reuse threshold.

The ceiling is equal to $2^{(\text{Max-suppress-time}/\text{Decay})} \times \text{reuse-limit}$. It is not user configurable.

Figure 1 shows the change rule of the penalty value. The lines $t_0$ and $t_2$ indicate the start time and end time of the suppression, respectively. The period from $t_0$ to $t_2$ indicates the suppression period, $t_0$ to $t_1$ indicates the max-suppress-time, and $t_1$ to $t_2$ indicates the complete decay period.
Configuration restrictions and guidelines

When you configure dampening on an Ethernet interface, follow these restrictions and guidelines:

- The `dampening`, `link-delay`, and `port link-flap protect enable` commands are mutually exclusive on an interface.
- The `dampening` command does not take effect on the administratively down events. When you execute the `shutdown` command, the penalty restores to 0, and the interface reports the down event to the upper-layer protocols.
- Do not enable the dampening feature on an interface with RRPP, MSTP, or Smart Link enabled.

Configuration procedure

To configure dampening on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>dampening [ half-life reuse suppress max-suppress-time ]</td>
<td>By default, interface dampening is disabled on Ethernet interfaces.</td>
</tr>
</tbody>
</table>

Enabling link flapping protection on an interface

About link flapping protection

Link flapping on an interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when interface status on the active link changes between UP and DOWN, traffic switches between active and standby links. To solve this problem, configure this feature on the interface.
With this feature enabled on an interface, when the interface goes down, the system enables link flapping detection. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Configuration restrictions and guidelines

This feature takes effect only when it is configured in both the system view and interface view.

The `dampening`, `link-delay`, and `port link-flap protect enable` commands are mutually exclusive on an Ethernet interface.

To bring up an interface that has been shut down by link flapping protection, execute the `undo shutdown` command.

In the `display interface` command output, the `Link-Flap DOWN` value of the `Current state` field indicates that the interface has been shut down by link flapping protection.

Configuration procedure

To enable link flapping protection on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enable link flapping protection on all interfaces.</td>
<td><code>link-flap protect enable</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enter Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>4.</td>
<td>Enable link flapping protection on an interface.</td>
<td>`port link-flap protect enable [ interval interval</td>
</tr>
</tbody>
</table>

Enabling loopback testing on an Ethernet interface

⚠ **CAUTION:**

After you enable this feature on an Ethernet interface, the interface cannot forward data traffic correctly.

Perform this task to determine whether an Ethernet link works correctly.

Loopback testing includes the following types:

- **Internal loopback testing**—Tests the device where the Ethernet interface resides. The Ethernet interface sends outgoing packets back to the local device. If the device fails to receive the packets, the device fails.
- **External loopback testing**—Tests the inter-device link. The Ethernet interface sends incoming packets back to the remote device. If the remote device fails to receive the packets, the inter-device link fails.

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.
- A loopback test cannot be performed on an interface configured with the `port up-mode` command.
- 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.
• In IRF 3.1, loopback testing enabled on an interface of the parent device is disabled until you execute the undo loopback command. Loopback testing enabled on an interface of a PEX is disabled after the test is performed for once. For more information about parent devices and PEXs, see Virtual Technologies Configuration Guide.

Configuration procedure

To enable loopback testing on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable loopback testing.</td>
<td>loopback { external</td>
</tr>
</tbody>
</table>

Configuring generic flow control on an Ethernet interface

To avoid dropping packets 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. Generic flow control includes the following types:

- **TxRx-mode generic flow control**—Enabled by using the flow-control command. 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 its peer, it suspends sending packets to its peer.

- **Rx-mode generic flow control**—Enabled by using the flow-control receive enable command. With Rx-mode generic flow control enabled, an interface can receive flow control frames, but it cannot send flow control frames:
  - When congestion occurs, the interface cannot send flow control frames to its peer.
  - When the interface receives a flow control frame from its peer, it suspends sending packets to its 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.

This feature is mutually exclusive with enabling PFC for 802.1p priorities.

To enable generic flow control on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.   | Enable generic flow control. | • Enable TxRx-mode generic flow control: flow-control  
• Enable Rx-mode generic flow control: flow-control receive enable | By default, generic flow control is disabled on an Ethernet interface. |
Configuring PFC on an Ethernet interface

When congestion occurs in the network, the local device notifies the peer to stop sending packets carrying the specified 802.1p priority if all of the following conditions exist:

- Both the local end and the remote end have PFC enabled.
- Both the local end and the remote end have the `priority-flow-control no-drop dot1p` command configured.
- The specified 802.1p priority is in the 802.1p priority list specified by the `dot1p-list` argument.
- The local end receives a packet carrying the specified 802.1p priority.

The state of the PFC feature is determined by the PFC configuration on the local end and on the peer end. In Table 1:

- The first row lists the PFC configuration on the local interface.
- The first column lists the PFC configuration on the peer.
- The `Enabled` and `Disabled` fields in other cells are possible negotiation results.

Make sure all interfaces that a data flow passes through have the same PFC configuration.

Table 1 PFC configurations and negotiation results

<table>
<thead>
<tr>
<th>Local (right)</th>
<th>Peer (below)</th>
<th>enable</th>
<th>auto</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>auto</td>
<td>Enabled</td>
<td>Enabled if negotiation succeeds. Enabled if negotiation fails.</td>
<td>Disabled</td>
</tr>
<tr>
<td>auto</td>
<td></td>
<td>Enabled</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Default</td>
<td></td>
<td>Disabled</td>
<td></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Configuration restrictions and guidelines

When you configure PFC, follow these restrictions and guidelines:

- For IRF and other protocols to operate correctly, as a best practice, do not enable PFC for 802.1p priorities 0, 6, and 7.
- To avoid packet loss, apply the same PFC configuration to all interfaces that the packets pass through.
- If you do not enable PFC on an interface, the interface can receive but cannot process PFC pause frames. To make PFC take effect, you must enable PFC on both ends.
- If you configure the `flow control` or `flow-control receive enable` command on a PFC-enabled interface, the following rules apply:
  - The PFC configuration takes effect.
  - The configuration of the `flow control` or `flow-control receive enable` command is ignored.
  - The `flow control` or `flow-control receive enable` command takes effect on the interface only when PFC is disabled on it.
- For PFC to take effect in an overlay network, execute the `qos trust tunnel-dot1p` command in system view. For information about the overlay network, see VXLAN Configuration Guide. For information about the `qos trust tunnel-dot1p` command, see priority mapping commands in ACL and QoS Command Reference.
- Enabling PFC for 802.1p priorities is mutually exclusive with generic flow control on an interface.
Configuration procedure

To configure PFC on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable PFC in auto mode or forcibly.</td>
<td>priority-flow-control { auto</td>
</tr>
<tr>
<td>4.</td>
<td>Enable PFC for 802.1p priorities.</td>
<td>priority-flow-control no-drop dot1p dot1p-list</td>
</tr>
</tbody>
</table>

Setting PFC thresholds

The storage spaces for an interface include the following types:

- Headroom storage space.
- Shared storage space.
- Guaranteed storage space.

Setting PFC thresholds enables flexible control over PFC and can make good use of the storage spaces. The switch supports the following PFC thresholds:

- **Headroom buffer threshold**—Maximum cell resources that can be used by packets with the specified 802.1p priority values in a headroom storage space. An interface drops received packets once this threshold is reached.

- **Back pressure frame triggering threshold**—Maximum cell resources that can be used by packets with the specified 802.1p priority values in a shared storage space. PFC is triggered once this threshold is reached. The back pressure frame triggering threshold includes the following types:
  - **Dynamic back pressure frame triggering threshold**—Maximum cell resources set in percentage.
  - **Static back pressure frame triggering threshold**—Maximum cell resources set in an absolute value.

- **Back pressure frame stopping threshold**—Number of cell resources that are used by packets with the specified 802.1p priority values. When this threshold is reached after PFC is triggered, PFC will be stopped.

- **PFC reserved threshold**—Number of cell resources reserved for packets with the specified 802.1p priority values in a guaranteed storage space.

Configuration restrictions and guidelines

⚠️ **CAUTION:**

After PFC for 802.1p priorities is enabled, each PFC threshold mentioned above uses a default value, which is adequate in typical network environments. As a practice, do not change the default value.

This feature is supported only in R2612 and later.

You must enable PFC for 802.1p priorities before setting the PFC thresholds.

If you cancel PFC threshold configurations on an interface, the PFC thresholds are restored to the state when only the **priority-flow-control no-drop dot1p** command is executed.
This feature does not support preprovisioning. For more information about preprovisioning, see *Fundamentals Configuration Guide*.

Enabling PFC for 802.1p priorities is mutually exclusive with generic flow control on an interface.

**Configuration procedure**

To set PFC thresholds:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the maximum cell resources that can be used in a headroom storage space.</td>
<td>priority-flow-control headroom headroom-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable PFC for 802.1p priorities.</td>
<td>priority-flow-control no-drop dot1p dot1p-list</td>
</tr>
<tr>
<td>5.</td>
<td>Set the headroom buffer threshold.</td>
<td>priority-flow-control dot1p dot1p headroom headroom-number</td>
</tr>
<tr>
<td>6.</td>
<td>Set the headroom buffer threshold.</td>
<td>• Set the dynamic back pressure frame triggering threshold: priority-flow-control dot1p dot1p ingress-buffer dynamic ratio&lt;br&gt;• Set the static back pressure frame triggering threshold: priority-flow-control dot1p dot1p ingress-buffer static threshold</td>
</tr>
<tr>
<td>7.</td>
<td>Set the back pressure frame stopping threshold.</td>
<td>priority-flow-control dot1p dot1p ingress-threshold-offset offset-number</td>
</tr>
<tr>
<td>8.</td>
<td>Set the PFC reserved threshold.</td>
<td>priority-flow-control dot1p dot1p reserved-buffer reserved-number</td>
</tr>
</tbody>
</table>

**Setting the statistics polling interval**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the statistics polling interval for the Ethernet interface.</td>
<td>flow-interval interval</td>
</tr>
</tbody>
</table>

To display the interface statistics collected in the last statistics polling interval, use the `display interface` command.
Configuring storm suppression

The storm suppression feature ensures that the size of a particular type of traffic (broadcast, multicast, or unknown unicast traffic) does not exceed the threshold 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. An interframe gap exists between each two continuous frames. The system excludes the time of interframe gaps in monitoring the traffic size on the interface. The configured suppression thresholds must be less than the total traffic that passes through the interface.

Both storm suppression and storm control can suppress storms on an interface. Storm suppression uses the chip to suppress traffic. Storm suppression has less impact on the device performance than storm control, which uses software to suppress traffic.

Configuration restrictions and guidelines

When you configure storm suppression, follow these restrictions and guidelines:

- For the traffic suppression result to be determined, do not configure storm control together with storm suppression for the same type of traffic. For more information about storm control, 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 device.
- Storm suppression configured on a Layer 3 Ethernet interface also takes effect on its subinterfaces if the interface is on the following networks:
  - Border of a VXLAN IP gateway network.
  - Border of an EVPN gateway network.

For more information about VXLAN IP gateway and EVPN gateway networks, see VXLAN Configuration Guide and EVPN Configuration Guide.

Configuration procedure

To set storm suppression thresholds on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable broadcast suppression and set the broadcast suppression threshold.</td>
<td>broadcast-suppression { ratio</td>
</tr>
<tr>
<td>4.</td>
<td>Enable multicast suppression and set the multicast suppression threshold.</td>
<td>multicast-suppression { ratio</td>
</tr>
<tr>
<td>5.</td>
<td>Enable unknown unicast suppression and set the unknown unicast suppression threshold.</td>
<td>unicast-suppression { ratio</td>
</tr>
</tbody>
</table>
Enabling remote fault signal detection

A fiber port forwards packets by using two optical fibers or only one optical fiber. Whether one optical fiber or two optical fibers are used by a fiber port depends on the fiber port model.

If a fiber port uses two optical fibers, one is used to receive packets, and the other one is used to send packets. The fiber port can go up and forward packets only when both optical fibers operate correctly. When the fiber port receives a remote fault signal, the physical state of the port becomes down. To keep the port in up state to operate correctly upon receiving a remote fault signal, disable remote fault signal detection on the port.

If a fiber port uses only one optical fiber, the physical state of the port becomes down when the port receives a remote fault signal. To keep the port in up state to operate correctly upon receiving a remote fault signal, disable remote fault signal detection on the port.

Configuration restrictions and guidelines

This feature is supported only in R2612 and later.

Only fiber ports support this feature.

Configuration procedure

To enable remote fault signal detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable remote fault signal detection.</td>
<td>link-fault-signal enable</td>
</tr>
</tbody>
</table>

Configuring a Layer 2 Ethernet interface

Configuring storm control on an Ethernet interface

About storm control

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 an upper threshold.

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

- **Blocks this type of traffic and forwards 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 interface begins to forward the traffic.
- **Goes down automatically**—The interface goes down automatically and stops forwarding any traffic. When the blocked traffic drops below the lower threshold, the interface does not automatically come up. To bring up the interface, use the undo shutdown command or disable the storm control feature.

You can configure an Ethernet interface to output threshold event traps and log messages when monitored traffic meets one of the following conditions:

- Exceeds the upper threshold.
- Drops below the lower threshold.
Both storm suppression and storm control can suppress storms on an interface. Storm suppression uses the chip to suppress traffic. Storm suppression has less impact on the device performance than storm control, which uses software to suppress traffic.

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 restrictions and guidelines**

For the traffic suppression result to be determined, do not configure storm control together with storm suppression for the same type of traffic. For more information about storm suppression, see "Configuring storm suppression."

**Configuration procedure**

To configure storm control on an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>storm-constrain interval interval</td>
<td>The default setting is 10 seconds. For network stability, use the default or set a longer statistics polling interval.</td>
</tr>
<tr>
<td>3.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>storm-constrain { broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td>5.</td>
<td>storm-constrain control { block</td>
<td>shutdown }</td>
</tr>
<tr>
<td>6.</td>
<td>storm-constrain enable log</td>
<td>By default, the Ethernet interface outputs log messages when monitored traffic exceeds the upper threshold or drops below the lower threshold.</td>
</tr>
<tr>
<td>7.</td>
<td>storm-constrain enable trap</td>
<td>By default, the Ethernet interface sends traps when monitored traffic exceeds the upper threshold or drops below the lower threshold from the upper threshold.</td>
</tr>
</tbody>
</table>

---

**Changing a Layer 2 Ethernet interface to an FC interface**

This feature allows you to change a Layer 2 Ethernet interface to an FC interface.

After you configure this feature on a Layer 2 Ethernet interface, the system deletes the interface, creates the FC interface, and enters FC interface view. This feature does not modify the interface number.

To change a Layer 2 Ethernet interface to an FC interface:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Change the Layer 2 Ethernet interface to an FC interface.</td>
<td>port-type fc</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Change the FC interface back to a Layer 2 Ethernet interface.</td>
<td>port-type ethernet</td>
</tr>
</tbody>
</table>

**Forcibly bringing up a fiber port**

**IMPORTANT:**
Copper ports do not support this feature.

As shown in Figure 2, a fiber port 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 forcibly brings up a fiber port, even when no fiber links or transceiver modules are present for the fiber port. When one fiber link is present and up, the fiber port can forward packets over the link unidirectionally.

**Figure 2** Forcibly bring up a fiber port

---

**Correct fiber connection**

**Device A**

**Device B**

**Fiber port**

**Tx end**

**Rx end**

---

**When Ethernet interfaces cannot be or are not forcibly brought up**

**Device A**

**Device B**

---

**When Ethernet interfaces are forcibly brought up**

**Device A**

**Device B**

---

- **Fiber port**
- **Tx end**
- **Rx end**
- **Fiber link**
- **Packets**
- **The fiber is disconnected.**
- **The interface is down.**
Configuration restrictions and guidelines

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

- The `shutdown` and `port up-mode` commands are mutually exclusive.
- The following operations on a fiber port will cause link updown events before the port finally stays up:
  - Configure both the `port up-mode` command and the `speed` or `duplex` command.
  - Install or remove fiber links or transceiver modules after you forcibly bring up the fiber port.
- Do not use this feature on a fiber port connected to a copper cable.

Configuration procedure

To forcibly bring up a fiber port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Forcibly bring up the fiber port.</td>
<td><code>port up-mode</code></td>
</tr>
</tbody>
</table>

Setting the MDIX mode of an Ethernet interface

**IMPORTANT:**
Fiber ports do not support the MDIX mode setting.

A physical Ethernet interface has 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.

**NOTE:**
This feature does not take effect on pins 4, 5, 7, and 8 of physical Ethernet interfaces.

- Pins 4, 5, 7, and 8 of interfaces operating at 10 Mbps or 100 Mbps do not receive or transmit signals.
- Pins 4, 5, 7, and 8 of interfaces operating at 1000 Mbps or higher rates receive and transmit signals.

To enable a copper Ethernet interface to communicate with its peer, set the MDIX mode of the interface by following these 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 device cannot determine the cable type.
- When a straight-through cable is used, configure the interface to operate in an MDIX mode different than its peer.
When a crossover cable is used, perform one of the following tasks:
  o  Configure the interface to operate in the same MDIX mode as its peer.
  o  Configure either end to operate in AutoMDIX mode.

To set the MDIX mode of an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the MDIX mode of the Ethernet interface.</td>
<td>mdix-mode { automdix</td>
</tr>
</tbody>
</table>

Testing the cable connection of an Ethernet interface

**IMPORTANT:**
If the link of an Ethernet interface is up, testing its cable connection will cause the link to go down and then come up.

**NOTE:**
Fiber ports do not support this feature.

This feature tests the cable connection of an Ethernet interface and displays cable test result within 5 seconds. The test result includes the cable’s status and some physical parameters. If any fault is detected, the test result shows the length from the local port to the faulty point.

To test the cable connection of an Ethernet interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
</tr>
<tr>
<td>3.</td>
<td>Perform a test for the cable connected to the Ethernet interface.</td>
</tr>
</tbody>
</table>

Enabling bridging on an Ethernet interface

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>port bridge enable</td>
<td>By default, bridging is disabled on an Ethernet interface.</td>
</tr>
</tbody>
</table>

Setting the interface connection distance

When two directly connected interfaces communicate, they use the buffer area to buffer the received data. A longer interface connection distance requires a greater buffer area.

Perform this task to modify the buffer area size by setting the interface connection distance.

To set the interface connection distance:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>port connection-distance { 300</td>
<td>10000</td>
</tr>
</tbody>
</table>

Configuring a Layer 3 Ethernet interface or subinterface

Setting the MTU for an Ethernet interface or subinterface

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

To set the MTU for an Ethernet interface or subinterface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type { interface-number</td>
<td>interface-number.subnumber }</td>
</tr>
<tr>
<td>3.</td>
<td>mtu size</td>
<td>The default setting is 1500 bytes.</td>
</tr>
</tbody>
</table>

Setting the MAC address of an Ethernet interface or subinterface

In a network, when the Layer 3 Ethernet interfaces or subinterfaces of different devices have the same MAC address, the devices might fail to communicate correctly. To eliminate the MAC address conflicts, use the mac-address command to modify the MAC addresses of Layer 3 Ethernet interfaces or subinterfaces.

The mac-address command cannot be executed on Layer 3 Ethernet interfaces or subinterfaces of border gateways in VXLAN IP gateway and EVPN gateway networks.
MAC addresses from the bridge MAC address of the device to the bridge MAC address plus 169 are reserved MAC addresses of the device. To avoid transmission failure, do not set the MAC address of an Ethernet interface or subinterface to one of the reserved MAC addresses. To avoid transmission failure after IRF master/subordinate switchover, do not set the MAC address of an Ethernet interface or subinterface to a reserved MAC address of an IRF member device. For more information about IRF bridge MAC addresses, see IRF in Virtual Technologies Configuration Guide.

To set the MAC address of an Ethernet interface or subinterface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface or subinterface view.</td>
<td>interface interface-type { interface-number | interface-number.subnumber }</td>
</tr>
<tr>
<td>3.</td>
<td>Set the MAC address of the Ethernet interface or subinterface.</td>
<td>mac-address mac-address</td>
</tr>
</tbody>
</table>

Enabling packet statistics for a Layer 3 Ethernet subinterface

⚠️ CAUTION:
This feature is resource intensive. When you use this feature, make sure you fully understand its impact on system performance.

In an EVPN network, after you enable this feature for a Layer 3 Ethernet subinterface, it cannot act as the outgoing interface of VXLAN tunnels.

To enable packet statistics for a Layer 3 Ethernet subinterface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 Ethernet subinterface view.</td>
<td>interface interface-type interface-number.subnumber</td>
</tr>
<tr>
<td>3.</td>
<td>Enable packet statistics for the Layer 3 Ethernet subinterface.</td>
<td>traffic-statistic enable</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Display the subinterface packet statistics.</td>
<td>• display counters • display interface</td>
</tr>
</tbody>
</table>

Displaying and maintaining an Ethernet interface or subinterface

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display interface traffic statistics.</td>
<td>display counters { inbound | outbound } interface { interface-type | interface-number }</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display traffic rate statistics of interfaces in up state over the</td>
<td>`display counters rate { inbound</td>
</tr>
<tr>
<td>last statistics polling interval.</td>
<td>interface-number.subnumber ] ]</td>
</tr>
<tr>
<td>Display the operational and status information of the specified</td>
<td><code>display interface</code> [interface-type [interface-number</td>
</tr>
<tr>
<td>interfaces.</td>
<td></td>
</tr>
<tr>
<td>Display information about link flapping protection on an interface.</td>
<td><code>display link-flap protection</code> [interface interface-type [interface-number ] ]</td>
</tr>
<tr>
<td>Display information about dropped packets on the specified interfaces.</td>
<td><code>display packet-drop</code> [interface [interface-type [interface-number ] ] [summary ] ]</td>
</tr>
<tr>
<td>Display the PFC information for an interface.</td>
<td><code>display priority-flow-control interface</code> [interface-type [interface-number ] ]</td>
</tr>
<tr>
<td>Display information about storm control on the specified interfaces.</td>
<td><code>display storm-constrain</code> [broadcast</td>
</tr>
<tr>
<td>Display the Ethernet module statistics.</td>
<td><code>display ethernet statistics</code> slot slot-number</td>
</tr>
<tr>
<td>Clear interface or subinterface statistics.</td>
<td><code>reset counters interface</code> [interface-type [interface-number</td>
</tr>
<tr>
<td>Clear the statistics of dropped packets on the specified interfaces.</td>
<td><code>reset packet-drop interface</code> [interface-type [interface-number ] ]</td>
</tr>
<tr>
<td>Clear the Ethernet module statistics.</td>
<td><code>reset ethernet statistics</code> [slot slot-number ]</td>
</tr>
</tbody>
</table>
Configuring loopback, null, and inloopback interfaces

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

Configuring a loopback interface

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

- **Configuring a loopback interface address as the source address of the IP packets that the device generates**—Because loopback interface addresses are stable unicast addresses, they are usually used as device identifications.
  - When you configure a rule on an authentication or security server to permit or deny packets that a device generates, you can simplify the rule by configuring it to permit or deny packets carrying the loopback interface address that identifies the device.
  - When you use a loopback interface address as the source address of IP packets, make sure the route from the loopback interface to the peer is reachable by performing routing configuration. All data packets sent to the loopback interface are considered packets sent to the device itself, so the device does not forward these packets.

- **Using a loopback interface in dynamic routing protocols**—With no router ID configured for a dynamic routing protocol, the system selects the highest loopback interface IP address as the router ID. In BGP, to avoid interruption of BGP sessions due to physical port failure, you can use a loopback interface as the source interface of BGP packets.

To configure a loopback interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface loopback interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>description text</td>
<td>The default setting is interface name Interface (for example, LoopBack1 Interface).</td>
</tr>
<tr>
<td>4.</td>
<td>bandwidth bandwidth-value</td>
<td>By default, the expected bandwidth of a loopback interface is 0 kbps.</td>
</tr>
<tr>
<td>5.</td>
<td>default</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td>undo shutdown</td>
<td>By default, a loopback interface is up.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter null interface view.</td>
<td>interface null 0</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the interface description.</td>
<td>description text</td>
</tr>
<tr>
<td>4.</td>
<td>Restore the default settings for the null interface.</td>
<td>default</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the specified or all loopback interfaces.</td>
<td>display interface loopback [ interface-number ] [ brief [ description</td>
</tr>
<tr>
<td>Display information about the null interface.</td>
<td>display interface null [ 0 ] [ brief [ description</td>
</tr>
<tr>
<td>Display information about the inloopback interface.</td>
<td>display interface inloopback [ 0 ] [ brief [ description</td>
</tr>
<tr>
<td>Clear the statistics on the specified or all loopback interfaces.</td>
<td>reset counters interface loopback [ interface-number ]</td>
</tr>
<tr>
<td>Clear the statistics on the null interface.</td>
<td>reset counters interface null [ 0 ]</td>
</tr>
</tbody>
</table>
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 commands supported by the first interface in the specified interface list are available for configuration.
- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the `interface interface-type { interface-number | interface-number.subnumber }` command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify in an interface range, the longer the command execution time.
- To guarantee bulk interface configuration performance, configure fewer than 1000 interface range names.
- After a command is executed in interface range view, one of the following situations might occur:
  - The system displays an error message and stays in interface range view. This means that the execution failed on one or multiple member interfaces.
    - If the execution failed on the first member interface, the command is not executed on any member interfaces.
    - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
  - The system returns to system view. This means that:
    - The command is supported in both system view and interface view.
    - The execution failed on a member interface in interface range view and succeeded in system view.
    - The command is not executed on the subsequent member interfaces.

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

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface range view.</td>
<td><code>interface range { interface-type interface-number { to interface-type interface-number } } &amp;&lt;1-24&gt;</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Display commands available for the first interface in the interface range. Enter a question mark (?) at the interface range prompt.</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>Use available commands to configure the interfaces. Available commands depend on the interface.</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Verify the configuration. display this</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Displaying and maintaining bulk interface configuration**

Execute the `display` command in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the interface ranges created by using the <code>interface range name</code> command.</td>
<td><code>display interface range [ name name ]</code></td>
</tr>
</tbody>
</table>
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 (or egress RB), 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.

The device performs the following operations to learn the source MAC address of incoming packets:
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 the incoming port if no entry is found.

When the device receives a frame destined for MAC-SOURCE after learning this source MAC address, the device performs the following operations:
3. Finds the MAC-SOURCE entry in the MAC address table.
4. Forwards the frame out of the port in the entry.

The device performs the learning process for each incoming 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, to block all frames destined for or sourced from a user, you can configure the MAC address of the user as a blackhole MAC address entry. A blackhole entry has higher priority than a dynamically learned one.

- **Multiport unicast entries**—A multiport unicast entry is manually added to send frames with a specific unicast destination MAC address out of multiple ports, and it never ages out. A multiport unicast entry has higher priority than a dynamically learned one.

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

Multiport unicast MAC address entries have no impact on the MAC address learning. When receiving a frame whose source MAC address matches a multiport unicast entry, the device can still learn the MAC address of the frame and generate a dynamic entry. However, the generated dynamic entry has lower priority. The device prefers to use the multiport unicast entry to forward frames destined for the MAC address in the entry.

### MAC address table configuration task list

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

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

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

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Configuring MAC address entries</td>
</tr>
<tr>
<td>• Adding or modifying a static or dynamic MAC address entry globally</td>
</tr>
<tr>
<td>• Adding or modifying a static or dynamic MAC address entry on an interface</td>
</tr>
<tr>
<td>• Adding or modifying a blackhole MAC address entry</td>
</tr>
<tr>
<td>• Adding or modifying a multiport unicast MAC address entry</td>
</tr>
<tr>
<td>(Optional.) Disabling MAC address learning</td>
</tr>
<tr>
<td>(Optional.) Setting the aging timer for dynamic MAC address entries</td>
</tr>
<tr>
<td>(Optional.) Setting the MAC learning limit</td>
</tr>
<tr>
<td>(Optional.) Configuring the unknown frame forwarding rule after the MAC learning limit is reached</td>
</tr>
<tr>
<td>(Optional.) Assigning MAC learning priority to interfaces</td>
</tr>
<tr>
<td>(Optional.) Enabling MAC address synchronization</td>
</tr>
<tr>
<td>(Optional.) Configuring MAC address move notifications and suppression</td>
</tr>
<tr>
<td>(Optional.) Enabling ARP fast update for MAC address moves</td>
</tr>
</tbody>
</table>
Configuring MAC address entries

Configuration guidelines

- A manually configured dynamic MAC address entry overwrites an existing learned entry 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.
- Do not configure the following MAC addresses as static, dynamic, blackhole, or multiport unicast MAC addresses:
  - Reserved MAC addresses of the device, which refer to MAC addresses from the bridge MAC address of the device to the bridge MAC address plus 169.
  - MAC addresses of Layer 3 Ethernet interfaces or subinterfaces.
  - MAC addresses of Layer 3 aggregate interfaces or subinterfaces.
- For packets to be correctly transmitted in the overlay network, do not configure multiport unicast MAC address entries for MAC addresses in the overlay network. For more information about overlay networks, see VXLAN Configuration Guide.

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static MAC address entry</td>
<td>Forwards the frame according to the destination MAC address regardless of whether the frame’s ingress interface is the same as that in the entry.</td>
</tr>
</tbody>
</table>
| Multiport unicast MAC address entry | • Learns the MAC address (MACA) of the frame and generates a dynamic MAC address entry, but the generated dynamic MAC address entry does not take effect.  
  • Forwards frames destined for MACA based on the multiport unicast MAC address entry. |
| Blackhole MAC address entry   | Drops the frame.                                                            |
| Dynamic MAC address entry     | • Learns the MAC address of the frames received on a different interface from that in the entry and overwrites the original entry.  
  • Forwards the frame received on the same interface as that in the entry and updates the aging timer for the entry. |

Adding or modifying a static or dynamic MAC address entry globally

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Adding or modifying a static or dynamic MAC address entry on an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Add or modify a static or dynamic MAC address entry.</td>
<td>mac-address { dynamic</td>
</tr>
</tbody>
</table>

### Adding or modifying a blackhole MAC address entry

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Add or modify a blackhole MAC address entry.</td>
<td>mac-address blackhole mac-address vlan vlan-id</td>
</tr>
</tbody>
</table>
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 (see Figure 3):

- All servers within a 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 to every server through all ports connected to the servers within the cluster.

![Figure 3 NLB cluster](image)

Figure 3 NLB cluster

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

**Configuring a multiport unicast MAC address entry globally**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Add or modify a multiport unicast MAC address entry.</td>
<td>mac-address multiport interface-list vlan vlan-id</td>
</tr>
</tbody>
</table>

**Configuring a multiport unicast MAC address entry on an interface**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>Enter Layer 2 Ethernet interface view: interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Add the interface to a</td>
<td>mac-address multiport</td>
</tr>
</tbody>
</table>
### 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.

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

### Disabling global MAC address learning

Global MAC address learning does not take effect on a TRILL network, S-channel, VPLS VSI, EVB VSI, or VXLAN VSI. For information about TRILL, see [TRILL Configuration Guide](#). For information about VPLS VSIs, see [MPLS Configuration Guide](#). For information about S-channels and EVB VSIs, see [EVB Configuration Guide](#). For information about VXLAN VSIs, see [VXLAN Configuration Guide](#).

To disable global MAC address learning:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable global MAC address learning.</td>
<td>undo mac-address mac-learning enable</td>
</tr>
</tbody>
</table>

### Disabling MAC address learning on interfaces

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

To disable MAC address learning on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 Ethernet interface view:</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface bridge-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface s-channel interface-number.channel-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel aggregate</td>
<td></td>
</tr>
</tbody>
</table>
### Disabling MAC address learning on a VLAN

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

To disable MAC address learning on a VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable global MAC address learning.</td>
<td>mac-address mac-learning enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>4.</td>
<td>Disable MAC address learning on the VLAN.</td>
<td>undo mac-address mac-learning enable</td>
</tr>
</tbody>
</table>

### Setting 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 its entries 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 set the aging timer for dynamic MAC address entries:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the aging timer for dynamic MAC address entries.</td>
<td>mac-address timer { aging seconds</td>
</tr>
</tbody>
</table>

### Setting the MAC learning limit

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

To set the MAC learning limit on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the MAC learning limit on the interface.</td>
<td>mac-address max-mac-count count</td>
</tr>
</tbody>
</table>

### Configuring the unknown frame forwarding rule after the MAC learning limit is reached

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

To configure the device to forward unknown frames received on the interface after the MAC learning limit on the interface is reached:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the device to forward unknown frames received on the interface after the MAC learning limit on the interface is reached.</td>
<td>mac-address max-mac-count enable-forwarding</td>
</tr>
</tbody>
</table>

### Assigning MAC learning priority to interfaces

The MAC learning priority mechanism assigns either low priority or high priority to an interface. An interface with high priority can learn MAC addresses as usual. However, an interface with low priority is not allowed to learn MAC addresses already learned on a high-priority interface.
The MAC learning priority mechanism can help defend your network against MAC address spoofing attacks. In a network that performs MAC-based forwarding, an upper layer device MAC address might be learned by a downlink interface because of a loop or attack to the downlink interface. To avoid this issue, perform the following tasks:

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

To assign MAC learning priority to an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface bridge-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface s-channel interface-number.channel-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface schannel-aggregation interface-number.channel-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel bundle interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface schannel-bundle interface-number</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Assign MAC learning priority to the interface.</td>
<td>By default, low MAC learning priority is used.</td>
</tr>
<tr>
<td></td>
<td>mac-address mac-learning priority { high</td>
<td>low }</td>
</tr>
</tbody>
</table>

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 4:
- 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.
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 5.

To enable MAC address synchronization:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable MAC address synchronization.</td>
<td>mac-address mac-roaming enable</td>
</tr>
</tbody>
</table>
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.

The MAC address move notifications feature enables the device to output MAC address move logs when MAC address moves are detected.

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

If the system detects that MAC address moves occur frequently on an interface, you can configure MAC address move suppression to shut the interface down. The interface automatically goes up after a suppression interval. Or, you can manually bring up the interface.

The MAC address move suppression feature must work with the ARP fast update for MAC address moves feature. For information about ARP fast update for MAC address moves, see "Enabling ARP fast update for MAC address moves."

To configure MAC address move notifications and MAC address move suppression:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enable MAC address move notifications and optionally specify a MAC move detection interval.</td>
<td><code>mac-address notification mac-move [ interval interval ]</code></td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Set MAC address move suppression parameters.</td>
<td><code>mac-address notification mac-move suppression { interval interval [ threshold threshold ] }</code></td>
</tr>
<tr>
<td>4.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Enter Layer 2 Ethernet interface view: `interface interface-type interface-number`
- Enter Layer 2 aggregate interface view: `interface bridge-aggregation interface-number`
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 6, 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 6 ARP fast update application scenario**

To enable ARP fast update for MAC address moves:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable ARP fast update for MAC address moves.</td>
<td>mac-address mac-move fast-update</td>
</tr>
</tbody>
</table>

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 device drops the frame.

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

To correctly forward traffic sourced from the MAC address of a VLAN interface, you must disable the static source check feature on the Layer 2 interfaces in the VLAN.

To disable the static source check feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>enter interface view.</td>
<td>undo mac-address static source-check enable</td>
</tr>
</tbody>
</table>

### Enabling SNMP notifications for the MAC address table

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For more information about SNMP and information center configuration, see the network management and monitoring configuration guide for the device.

To enable SNMP notifications for the MAC address table:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>enable SNMP notifications for the MAC address table.</td>
<td>snmp-agent trap enable mac-address [ mac-move ]</td>
</tr>
</tbody>
</table>
Displaying and maintaining the MAC address table

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display MAC address table information.</td>
<td>`display mac-address [ mac-address [ vlan vlan-id ] [ [ dynamic</td>
</tr>
<tr>
<td>Display the aging timer for dynamic MAC address entries.</td>
<td><code>display mac-address aging-time</code></td>
</tr>
<tr>
<td>Display the system or interface MAC address learning state.</td>
<td><code>display mac-address mac-learning [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Display MAC address statistics.</td>
<td><code>display mac-address statistics</code></td>
</tr>
<tr>
<td>Display the MAC address move records.</td>
<td><code>display mac-address mac-move [ slot slot-number ]</code></td>
</tr>
</tbody>
</table>

MAC address table configuration example

Network requirements

As shown in Figure 7:
- Host A at MAC address 000f-e235-dc71 is connected to Ten-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 Host B.
- Set the aging timer to 500 seconds for dynamic MAC address entries.

Figure 7 Network diagram

![Network diagram](image-url)
Configuration procedure

# Add a static MAC address entry for MAC address 000f-e235-dc71 on Ten-GigabitEthernet 1/0/1 that belongs to VLAN 1.
<Device> system-view
[Device] mac-address static 000f-e235-dc71 interface ten-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 Ten-GigabitEthernet 1/0/1.
[Device] display mac-address static interface ten-gigabitethernet 1/0/1
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLAN ID</th>
<th>State</th>
<th>Port/Nickname</th>
<th>Aging</th>
</tr>
</thead>
<tbody>
<tr>
<td>000f-e235-dc71</td>
<td>1</td>
<td>Static</td>
<td>XGE1/0/1</td>
<td>N</td>
</tr>
</tbody>
</table>

# Display the blackhole MAC address entries.
[Device] display mac-address blackhole
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLAN ID</th>
<th>State</th>
<th>Port/Nickname</th>
<th>Aging</th>
</tr>
</thead>
<tbody>
<tr>
<td>000f-e235-abcd</td>
<td>1</td>
<td>Blackhole</td>
<td>N/A</td>
<td>N</td>
</tr>
</tbody>
</table>

# 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 user's 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.

Enabling MAC Information

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable MAC Information globally.</td>
<td>mac-address information enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Enable MAC Information on the interface.</td>
<td>mac-address information enable { added | deleted }</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the MAC Information mode.</td>
<td>mac-address information mode ( syslog</td>
</tr>
</tbody>
</table>

**Setting 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the MAC change notification interval.</td>
<td>mac-address information interval interval</td>
</tr>
</tbody>
</table>

**Setting the MAC Information queue length**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the MAC Information queue length.</td>
<td>mac-address information queue-length value</td>
</tr>
</tbody>
</table>

**MAC Information configuration example**

**Network requirements**

Enable MAC Information on Ten-GigabitEthernet 1/0/1 on Device in *Figure 8* to send MAC address changes in syslog messages to the log host, Host B, through interface Ten-GigabitEthernet 1/0/2.
Figure 8 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 no lower than 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
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 no lower than **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 Ten-GigabitEthernet 1/0/1 to enable the port 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 ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] mac-address information enable added
[Device-Ten-GigabitEthernet1/0/1] mac-address information enable deleted
[Device-Ten-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

Overview

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.

Ethernet link aggregation application scenario

As shown in Figure 9, 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 transmitted on the failed link is switched to the other two links.

Ethernet link aggregation can also aggregate the S-channels created on Ethernet interfaces for connections with an EVB server. For more information about S-channels, see *EVB Configuration Guide*.

Figure 9 Ethernet link aggregation diagram

Aggregation group, member port, and aggregate interface

Each link aggregation is represented by a logical aggregate interface. Each aggregate interface has an automatically created aggregation group, which contains member ports to be used for aggregation. The type and number of an aggregation group are the same as its aggregate interface.

Supported aggregate interface types

An aggregate interface can be one of the following types:

- **Layer 2**—A Layer 2 aggregate interface is created manually. The member ports in a Layer 2 aggregation group can only be Layer 2 Ethernet interfaces.

  On an IRF 3.1 system, an aggregation group is called a Layer 2 extended-link aggregation group if its member ports are on PEXs. The logical interface of the aggregation group is called a Layer 2 extended-link aggregate interface. For more information about PEXs, see IRF 3.1 configuration in *Virtual Technologies Configuration Guide*.

- **Layer 3**—A Layer 3 aggregate interface is created manually. The member ports in its Layer 3 aggregation group can only be Layer 3 Ethernet interfaces.

  On a Layer 3 aggregate interface, you can create subinterfaces. A Layer 3 aggregate subinterface processes traffic only for the VLAN numbered with the same ID as the subinterface number.
- **S-channel bundle**—An S-channel bundle interface is created manually. The member ports in an S-channel bundle group can only be S-channel interfaces.

**NOTE:**
The term "S-channel interface" in Ethernet link aggregation refers to the S-channel interface of an S-channel created on an Ethernet interface.

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 Selected member ports, see "Aggregation states of member ports in an aggregation group."

### Aggregation states of member ports in an aggregation group

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

- **Selected**—A Selected port can forward traffic.
- **Unselected**—An Unselected port cannot forward traffic.
- **Individual**—An Individual port can forward traffic as a normal physical port. A port is placed in the Individual state when the following conditions exist:
  - Its aggregate interface is configured as an edge aggregate interface.
  - The port has not received Link Aggregation Control Protocol Data Units (LACPDUs) from its peer port.

### Operational key

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

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

### Configuration types

Port configurations include attribute configurations and protocol configurations. Attribute configurations of a link aggregation member port affect its aggregation state.

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

  Attribute configuration changes made on an aggregate interface are automatically synchronized to all member ports. If the changes fail to be synchronized to a Selected port, the port might change to the Unselected state. To make the port become Selected again, you can change the attribute configurations on the aggregate interface or the member port. The synchronization failure does not affect the attribute configuration changes made on the aggregate interface. The configurations that have been synchronized from the aggregate interface are retained on the member ports even after the aggregate interface is deleted.

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

**Table 2 Attribute configurations**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port isolation</td>
<td>Indicates whether the port has joined an isolation group and which isolation group the port belongs to.</td>
</tr>
</tbody>
</table>
### Feature Considerations

<table>
<thead>
<tr>
<th>Feature</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>QinQ</td>
<td>QinQ status (enabled/disabled), TPID for VLAN tags, and VLAN transparent transmission. For information about QinQ, see &quot;Configuring QinQ.&quot;</td>
</tr>
<tr>
<td>VLAN mapping</td>
<td>VLAN mapping configured on the port. For more information about VLAN mapping, see &quot;Configuring VLAN mapping.&quot;</td>
</tr>
</tbody>
</table>
| VLAN             | VLAN attribute configurations include the following:  
|                  | • Permitted VLAN IDs.  
|                  | • PVID.  
|                  | • Link type (trunk, hybrid, or access).  
|                  | • PVLAN port type (promiscuous, trunk promiscuous, host, or trunk secondary).  
|                  | • IP subnet-based VLAN configuration.  
|                  | • Protocol-based VLAN configuration.  
|                  | • VLAN tagging mode.  
|                  | For information about VLANs, see "Configuring VLANs."                                                                                                                                                                                                                               |

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

**NOTE:**
- The protocol configurations for an aggregate interface take effect only on the current aggregate interface.
- The protocol configurations for a member port take effect only when the port leaves its aggregation group.

### Link aggregation modes

An aggregation group operates in one of the following modes:
- **Static**—Static aggregation is stable. An aggregation group in static mode is called a static aggregation group. The aggregation states 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.

### How static link aggregation works

#### Choosing a reference port

When setting the aggregation states 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 in up state.

The candidate reference ports are organized into different priority levels following these rules:
1. In descending order of port priority.
2. Full duplex.
3. In descending order of speed.
4. Half duplex.
5. In descending order of speed.

From the candidate ports with the same attribute configurations as the aggregate interface, the one with the highest priority level is chosen as the reference port.

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

**Setting the aggregation state of each member port**

After the reference port is chosen, the system sets the aggregation state of each member port in the static aggregation group.

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

After the limit on Selected ports is reached, the aggregation state of a new member port varies by following conditions:

- The port is placed in Unselected state if the port and the Selected ports have the same port priority. This mechanism prevents traffic interruption on the existing Selected ports. A device reboot can cause the device to recalculate the aggregation states of member ports.
- The port is placed in Selected state when the following conditions are met:
  - The port and the Selected ports have different port priorities, and the port has a higher port priority than a minimum of one Selected port.
The port has the same attribute configurations as the aggregate interface. Any operational key or attribute configuration change might affect the aggregation states of link aggregation member ports.

Dynamic link aggregation

Methods to assign interfaces to a dynamic link aggregation group

You can use one of the following methods to assign interfaces to a dynamic link aggregation group:

- **Manual assignment**—Manually assign interfaces to the dynamic link aggregation group.
- **Automatic assignment**—Enable automatic assignment on interfaces to have them automatically join a dynamic link aggregation group depending on the peer information in the received LACPDUs.

**NOTE:**
When you use automatic assignment on one end, you must use manual assignment on the other end.

LACP

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

LACP uses LACPDUs to exchange aggregation information between LACP-enabled devices. Each member port in a dynamic aggregation group can exchange 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 Selected state.

LACP functions

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic LACP functions</td>
<td>Implemented through the basic LACPDU fields, including the LACP system priority, system MAC address, port priority, port number, and operational key.</td>
</tr>
<tr>
<td>Extended LACP functions</td>
<td>Implemented by extending the LACPDU with new TLV fields. Extended LACP can implement LACP MAD for the IRF feature. 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 Virtual Technologies Configuration Guide.</td>
</tr>
</tbody>
</table>

LACP operating modes

LACP can operate in active or passive mode.

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

LACP priorities

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System LACP priority</td>
<td>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 LACP system priority sets the Selected state of member ports on its side. The system that has lower priority sets the aggregation state of local member ports the same as their respective peer ports.</td>
</tr>
<tr>
<td>Port priority</td>
<td>Determines the likelihood of a member port to be a Selected port on a system. A port with a higher port priority is more likely to become Selected.</td>
</tr>
</tbody>
</table>

### 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 has not received LACPDUs from the peer within the LACP timeout interval, the member port considers the peer as failed.

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

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

### Automatic member interface assignment

As shown in Figure 11, an interface enabled with automatic assignment joins a dynamic aggregation group based on the peer information in the LACPDUs received from the aggregation peer. If none of the existing dynamic aggregation groups is qualified, the device automatically creates a new dynamic aggregation group.

In a dynamic aggregation group that contains both automatically added member ports, the device selects a reference port preferentially from the manually added member ports. The device selects a reference port from automatically added member ports only when manually added member ports are not available.
How dynamic link aggregation works

Choosing a reference port

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

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

1. The two systems determine the system with the smaller system ID.
   
   A system ID contains the LACP system priority and the system MAC address.
   
   a. The two systems compare their LACP priority values.
      
      The lower the LACP priority, the smaller the system ID. If the LACP priority values are the same, the two systems proceed to step b.
   
   b. The two systems compare their MAC addresses.
      
      The lower the MAC address, the smaller the system ID.

2. The system with the smaller system ID chooses the port with the smallest port ID as the reference port.
   
   A port ID contains a port priority and a port number. The lower the port priority, the smaller the port ID.
   
   a. The system chooses the port with the lowest priority value as the reference port.
      
      If the ports have the same priority, the system proceeds to step b.
   
   b. The system compares their port numbers.
      
      The smaller the port number, the smaller the port ID.
      
      The port with the smallest port number and the same attribute configurations as the aggregate interface is chosen as the reference port.
Setting the aggregation state of each member port

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

Figure 12 Setting the state of a member port in a dynamic aggregation group

The system with the greater system ID can detect the aggregation state changes on the peer system. The system with the greater system ID 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 chooses only full-duplex ports as the Selected ports.
- For stable aggregation and service continuity, do not change the operational key or attribute configurations on any member port.
- After the Selected port limit is reached, a newly joining port becomes a Selected port if it is more eligible than a current Selected port.
Edge aggregate interface

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

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

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

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

Load sharing modes for link aggregation groups

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

- **Per-flow load sharing**—Load shares traffic on a per-flow basis. The load sharing mode classifies packets into flows and forwards packets of the same flow on the same link. This mode can be one or any combination of the following traffic classification criteria:
  - Ingress port.
  - Source or destination IP address.
  - Source or destination MAC address.
  - Source or destination port number.

- **Packet type-based load sharing**—Load shares traffic automatically based on packet types (Layer 2 protocol, IPv4, or IPv6).

S-MLAG

**IMPORTANT:**

This feature is supported in R2612 and later.

Simple multichassis link aggregation (S-MLAG) enhances dynamic link aggregation to establish an aggregation that spans multiple devices to a remote device.

An S-MLAG multichassis aggregation connects one dynamic Layer 2 aggregate interface on each S-MLAG device to the remote device, as shown in Figure 13.

S-MLAG uses an S-MLAG group to manage the aggregate interfaces for each aggregation, and it runs LACP to maintain each aggregation as does dynamic link aggregation. To the remote device, the S-MLAG devices appear as one peer aggregation system.
Figure 13 S-MLAG application scenario

Tasks at a glance

(Required.) Configuring an aggregation group:
- Configuring a Layer 2 aggregation group
- Configuring a Layer 3 aggregation group
- Configuring an S-channel bundle group

(Optional.) Configuring an aggregate interface:
- Configuring the description of an aggregate interface
- Changing the MAC address of a Layer 3 aggregate interface or subinterface
- Specifying ignored VLANs for a Layer 2 aggregate interface
- Ignoring port speed in setting the aggregation states of member ports
- Setting the MTU for a Layer 3 aggregate interface
- Setting the minimum and maximum numbers of Selected ports for an aggregation group
- Setting the expected bandwidth for an aggregate interface
- Configuring an edge aggregate interface
- Enabling BFD for an aggregation group
- Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection
- Shutting down an aggregate interface
- Enabling packet statistics for a Layer 3 aggregate subinterface
- Restoring the default settings for an aggregate interface

(Optional.) Configuring load sharing for link aggregation groups:
- Setting load sharing modes for link aggregation groups
- Specifying ignored packet fields for default link-aggregation load sharing
- Enabling local-first load sharing for link aggregation
- Configuring link aggregation load sharing algorithm settings
- Setting the global load sharing mode for MAC-in-MAC traffic

(Optional.) Enabling link-aggregation traffic redirection

(Optional.) Specifying link aggregation management VLANs and management port

(Optional.) Excluding a subnet from load sharing on aggregate links

(Optional.) Enabling a Layer 2 aggregate interface to reflect incoming packets back

(Optional.) Enabling transparent LACPDU transmission
Tasks at a glance
(Optional.) Configuring S-MLAG

Configuring an aggregation group

This section explains how to configure an aggregation group.

Configuration restrictions and guidelines for link aggregation configuration

The following information describes restrictions and guidelines that you must follow when you configure link aggregations.

Aggregation member interface restrictions

- You cannot assign an interface to a Layer 2 aggregation group if any features in Table 5 are configured on the interface.

<table>
<thead>
<tr>
<th>Feature on the interface</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC authentication</td>
<td>MAC authentication in Security Configuration Guide</td>
</tr>
<tr>
<td>Port security</td>
<td>Port security in Security Configuration Guide</td>
</tr>
<tr>
<td>802.1X</td>
<td>802.1X in Security Configuration Guide</td>
</tr>
</tbody>
</table>

- Do not assign a reflector port for port mirroring to an aggregation group. For more information about reflector ports, see Network Management and Monitoring Configuration Guide.
- A Layer 2 extended-link aggregation group can contain only extended ports that are on the PEXs in the same PEX group and at the same tier.

Configuration consistency requirements

- You must configure the same aggregation mode at the two ends of an aggregate link.
- For a successful static aggregation, make sure the ports at both ends of each link are in the same aggregation state.
- For a successful dynamic aggregation:
  - Make sure 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.
  - If you use automatic interface assignment on one end, you must use manual assignment on the other end.

Layer 3 aggregate subinterface restrictions

If you associate a VPN instance with a Layer 3 aggregate subinterface, you must also perform one or both of the following tasks:

- Associate the VPN instance with the following interfaces:
  - The Layer 3 Ethernet subinterfaces that have the same subinterface number as the Layer 3 aggregate subinterface.
  - The VLAN interface that has the same number as the subinterface number of the Layer 3 aggregate subinterface.
- Enable packet statistics for the Layer 3 aggregate subinterface.
For more information about Layer 3 Ethernet subinterfaces, see "Configuring Ethernet interfaces."
For more information about VLAN interfaces, see "Configuring VLANs."
For more information about VPN instance configuration for interfaces, see MPLS L3VPN and MCE configuration in MPLS Configuration Guide.

**Miscellaneous**

Deleting an aggregate interface also deletes its aggregation group and causes all member ports to leave the aggregation group.

**Configuring a Layer 2 aggregation group**

**Configuring a Layer 2 static aggregation group**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.</td>
<td>interface bridge-aggregation interface-number [ pex ]</td>
</tr>
<tr>
<td>3.</td>
<td>Exit to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Assign an interface to a Layer 2 aggregation group.</td>
<td>a Enter Layer 2 Ethernet interface view: interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>b Assign the interface to the specified Layer 2 aggregation group: port link-aggregation group group-id [ force ]</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Set the port priority for the interface.</td>
<td>link-aggregation port-priority priority</td>
</tr>
</tbody>
</table>

**Configuring a Layer 2 dynamic aggregation group**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the LACP system priority.</td>
<td>lACP system-priority priority</td>
</tr>
<tr>
<td>3.</td>
<td>Create a Layer 2 aggregate interface and enter Layer 2</td>
<td>interface bridge-aggregation interface-number [ pex ]</td>
</tr>
</tbody>
</table>
### Configuring a Layer 2 aggregation group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate interface view.</td>
<td>link-aggregation mode dynamic</td>
<td>automatically creates a Layer 2 static aggregation group numbered the same. To create a Layer 2 extended-link aggregate interface, specify the <code>pex</code> keyword. Do not specify the <code>pex</code> keyword when you create Layer 2 aggregate interface Bridge-Aggregation 1.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the aggregation group to operate in dynamic mode.</td>
<td>By default, an aggregation group operates in static mode.</td>
</tr>
<tr>
<td>5.</td>
<td>Exit to system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td>Assign an interface to a Layer 2 aggregation group or enable automatic assignment on that interface.</td>
<td>a Enter Layer 2 Ethernet interface view: interface interface-type interface-number b Assign the interface to a Layer 2 aggregation group or configure automatic assignment: port link-aggregation group { group-id</td>
</tr>
<tr>
<td>7.</td>
<td>Set the LACP operating mode for the interface.</td>
<td>• Set the LACP operating mode to passive: lacp mode passive • Set the LACP operating mode to active: undo lacp mode By default, LACP is operating in active mode.</td>
</tr>
<tr>
<td>8.</td>
<td>Set the port priority for the interface.</td>
<td>link-aggregation port-priority priority The default setting is 32768.</td>
</tr>
<tr>
<td>9.</td>
<td>Set the short LACP timeout interval (3 seconds) for the interface.</td>
<td>lACP period short By default, the long LACP timeout interval (90 seconds) is used by the interface. To avoid traffic interruption during an ISSU, do not set the short LACP timeout interval before performing the ISSU. For more information about ISSU, see Fundamentals Configuration Guide.</td>
</tr>
</tbody>
</table>

### Configuring a Layer 3 aggregation group

#### Configuring a Layer 3 static aggregation group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Create a Layer 3 aggregate interface and enter Layer 3</td>
<td>interface route-aggregation interface-number When you create a Layer 3 aggregate interface, the system</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>aggregate interface view.</td>
<td></td>
<td>automatically creates a Layer 3 static aggregation group numbered the same.</td>
</tr>
<tr>
<td>3.</td>
<td>Exit to system view. quit</td>
<td>N/A</td>
</tr>
<tr>
<td>4. Assign an interface to a Layer 3 aggregation group.</td>
<td>a Enter Layer 3 Ethernet interface view: <code>interface interface-type interface-number</code> b Assign the interface to the specified Layer 3 aggregation group: <code>port link-aggregation group group-id</code></td>
<td>Repeat these two substeps to assign more Layer 3 Ethernet interfaces to the aggregation group.</td>
</tr>
<tr>
<td>5. (Optional.) Set the port priority for the interface.</td>
<td>link-aggregation port-priority priority</td>
<td>The default port priority of an interface is 32768.</td>
</tr>
</tbody>
</table>

### Configuring a Layer 3 dynamic aggregation group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the LACP system priority.</td>
<td><code>lacp system-priority priority</code></td>
<td>By default, the LACP system priority is 32768. Changing the LACP system priority might affect the aggregation states of the ports in the dynamic aggregation group.</td>
</tr>
<tr>
<td>3. Create a Layer 3 aggregate interface and enter Layer 3 aggregate interface view.</td>
<td><code>interface route-aggregation interface-number</code></td>
<td>When you create a Layer 3 aggregate interface, the system automatically creates a Layer 3 static aggregation group numbered the same.</td>
</tr>
<tr>
<td>4. Configure the aggregation group to operate in dynamic mode.</td>
<td><code>link-aggregation mode dynamic</code></td>
<td>By default, an aggregation group operates in static mode.</td>
</tr>
<tr>
<td>5. Exit to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>6. Assign an interface to a Layer 3 aggregation group or enable automatic assignment on that interface.</td>
<td>a Enter Layer 3 Ethernet interface view: <code>interface interface-type interface-number</code> b Assign the interface to a Layer 3 aggregation group or configure automatic assignment: `port link-aggregation group { group-id</td>
<td>auto [ group-id ]}`</td>
</tr>
<tr>
<td>7. Set the LACP operating mode for the interface.</td>
<td>• Set the LACP operating mode to passive: <code>lacp mode passive</code> • Set the LACP operating mode to active: <code>undo lacp mode</code></td>
<td>By default, LACP is operating in active mode.</td>
</tr>
<tr>
<td>8. Set the port priority for the interface.</td>
<td><code>link-aggregation port-priority priority</code></td>
<td>The default setting is 32768.</td>
</tr>
</tbody>
</table>
### Configuring an S-channel bundle group

#### Configuring a static S-channel bundle group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an S-channel bundle interface and enter S-channel bundle interface view.</td>
<td>interface schannel-bundle interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Exit to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Assign an S-channel interface to an S-channel bundle group.</td>
<td>a) Enter S-channel interface view: <code>interface s-channel interface-number:channel-id</code>&lt;br&gt;b) Assign the interface to the specified S-channel bundle group: <code>port link-aggregation group group-id [ force ]</code></td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Set the port priority for the interface.</td>
<td>a) <code>link-aggregation port-priority priority</code></td>
</tr>
</tbody>
</table>

#### Configuring a dynamic S-channel bundle group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the LACP system priority.</td>
<td>lACP system-priority <code>priority</code></td>
</tr>
<tr>
<td>3.</td>
<td>Create an S-channel bundle interface and enter S-channel bundle</td>
<td>interface schannel-bundle interface-number</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>interface view.</td>
<td></td>
<td>S-channel bundle group numbered the same.</td>
</tr>
<tr>
<td>4.</td>
<td>link-aggregation mode dynamic</td>
<td>By default, an S-channel bundle group operates in static mode.</td>
</tr>
<tr>
<td>5.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td><strong>a</strong> Enter S-channel interface view: interface s-channel interface-number.channel-id <strong>b</strong> Assign the interface to the specified S-channel bundle group: port link-aggregation group group-id [ force ]</td>
<td>Repeat these two substeps to assign more S-channel interfaces to the bundle group. To synchronize the attribute configurations from the aggregate interface when the current interface joins the aggregation group, you must specify the <strong>force</strong> keyword. For more information about EVB, see <strong>EVB Configuration Guide</strong>.</td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td>By default, LACP is operating in active mode.</td>
</tr>
<tr>
<td>8.</td>
<td>link-aggregation port-priority priority</td>
<td>The default port priority of an interface is 32768.</td>
</tr>
<tr>
<td>9.</td>
<td>lACP period short</td>
<td>By default, the long LACP timeout interval (90 seconds) is used by the interface. To avoid traffic interruption during an ISSU, do not set the short LACP timeout interval before performing the ISSU. For more information about ISSU, see <strong>Fundamentals Configuration Guide</strong>.</td>
</tr>
</tbody>
</table>

### Configuring an aggregate interface

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

### Configuring the description of an aggregate interface

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

To configure the description of an aggregate interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter aggregate interface or subinterface</td>
<td>Enter Layer 2 aggregate interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>view.</td>
<td>interface bridge-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td>• Enter Layer 3 aggregate interface or subinterface view:</td>
<td>interface route-aggregation { interface-number</td>
<td>interface-number.subnumber }</td>
</tr>
<tr>
<td>• Enter S-channel bundle interface view:</td>
<td>interface schannel-bundle interface-number</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the description of the aggregate interface or subinterface.</td>
<td>description text</td>
</tr>
</tbody>
</table>

### Changing the MAC address of a Layer 3 aggregate interface or subinterface

By default, all Layer 3 aggregate interfaces and subinterfaces on a device use the same MAC address. The default MAC address of Layer 3 aggregate interfaces and subinterfaces varies by device.

Do not use this command on a border gateway of a VXLAN or EVPN network.

The bridge MAC address of the device and its subsequent higher 169 consecutive MAC addresses are reserved. To avoid forwarding failure, do not assign a reserved MAC address to an aggregate interface or subinterface.

To avoid forwarding failure after an IRF master/subordinate switchover, do not assign the IRF bridge MAC address to an aggregate interface or subinterface. For more information about the IRF bridge MAC address, see Virtual Technologies Configuration Guide.

To change the MAC address of an aggregate interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 aggregate interface or subinterface view.</td>
<td>interface route-aggregation { interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Change the MAC address of the aggregate interface.</td>
<td>mac-address mac-address</td>
</tr>
</tbody>
</table>

### Specifying ignored VLANs for a Layer 2 aggregate interface

This feature takes effect only when the link type of a Layer 2 aggregate interface is hybrid or trunk.
To become Selected, the member ports by default must have the same VLAN permit state and tagging mode as the Layer 2 aggregate interface.

This feature enables the system to ignore the permit state and tagging mode of an ignored VLAN when choosing Selected ports.

To specify ignored VLANs for a Layer 2 aggregate interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 aggregate interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Specify ignored VLANs.</td>
<td>By default, a Layer 2 aggregate interface does not ignore any VLANs.</td>
</tr>
</tbody>
</table>

Ignoring port speed in setting the aggregation states of member ports

This feature allows ports at a different speed than the reference port to become Selected by ignoring the port speed during operational key calculation.

You must configure the same port speed ignoring setting at the two ends of a static configuration to ensure that the peer ports are placed in the same aggregation state. This requirement does not apply to a dynamic aggregation, on which the two ends negotiate the aggregation state of the peer ports automatically.

To configure an aggregation group to ignore port speed in setting the aggregation states of member ports:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter aggregate interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the aggregation group to ignore port speed in setting the aggregation states of member ports.</td>
<td>By default, an aggregation group does not ignore port speed in setting the aggregation states of member ports.</td>
</tr>
</tbody>
</table>

Setting the MTU for a Layer 3 aggregate interface

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

To set the MTU for a Layer 3 aggregate interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 aggregate interface or subinterface view.</td>
<td>interface route-aggregation { interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the MTU for the Layer 3 aggregate interface or subinterface.</td>
<td>mtu size</td>
</tr>
</tbody>
</table>

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

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

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 states of aggregation member ports and the state of the aggregate interface.

- When the number of member ports eligible to be Selected ports is smaller than the minimum threshold, the following events occur:
  - The eligible member ports are placed in Unselected state.
  - The link layer state of the aggregate interface becomes down.
- When the number of member ports eligible to be Selected ports reaches or exceeds the minimum threshold, the following events occur:
  - The eligible member ports are placed in Selected state.
  - The link layer state of the aggregate interface becomes up.

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

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

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

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

Configuration restrictions and guidelines

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

Configuration procedure

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter aggregate interface view.</td>
<td>• Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter Layer 3 aggregate interface view:</td>
</tr>
</tbody>
</table>

64
### Setting the expected bandwidth for an aggregate interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter aggregate interface view.</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the expected bandwidth for the interface.</td>
<td>bandwidth bandwidth-value</td>
<td>By default, the expected bandwidth (in kbps) is the interface baud rate divided by 1000.</td>
</tr>
</tbody>
</table>

### Configuring an edge aggregate interface

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

- This configuration takes effect only on the aggregate interface corresponding to a dynamic aggregation group.

- Link-aggregation traffic redirection does not operate correctly on an edge aggregate interface. For more information about link-aggregation traffic redirection, see “Enabling link-aggregation traffic redirection.”

To configure an edge aggregate interface:
### Enabling BFD for an aggregation group

#### About BFD for Ethernet link aggregation

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

- **BFD on a 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 then placed in Unselected state. However, the BFD session between the local and peer ports remains, and the local port keeps sending BFD packets. When BFD on the local port receives packets from the peer port upon link recovery, BFD notifies the Ethernet link aggregation module that the peer port is reachable. Then, the local port is placed in Selected state again. This mechanism ensures that the local and peer ports of a static aggregate link have the same aggregation state.

- **BFD on a dynamic aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. At the same time, BFD clears the session and stops sending BFD packets. When the local port is placed in Selected state again upon link recovery, the local port establishes a new session with the peer port and BFD notifies the Ethernet link aggregation module that the peer port is reachable. Because BFD provides fast failure detection, the local and peer systems of a dynamic aggregate link can negotiate the aggregation state of their member ports faster.

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

#### Configuration restrictions and guidelines

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

- Make sure the source and destination IP addresses are consistent at the two ends of an aggregate link. For example, if you execute `link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2` on the local end, execute `link-aggregation bfd ipv4 source 2.2.2.2 destination 1.1.1.1` on the peer end. The source and destination IP addresses cannot be the same.

- The BFD parameters configured on an aggregate interface take effect on all BFD sessions established by the member ports in its aggregation group. BFD on a link aggregation supports only control packet mode for session establishment and maintenance. The two ends of an established BFD session can only operate in Asynchronous mode.
- As a best practice, do not configure BFD for any protocols on a BFD-enabled aggregate interface.

- Make sure the number of member ports in a BFD-enabled aggregation group is less than or identical to the number of BFD sessions supported by the device. If the aggregation group contains more member ports than the supported sessions, some Selected ports might change to the Unselected state.

- If the number of BFD sessions differs between the two ends of an aggregate link, check their settings for inconsistency in the maximum number of Selected ports. You must make sure the two ends have the same setting for the maximum number of Selected ports.

**Configuration procedure**

To enable BFD for an aggregation group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter aggregate interface view. | • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number  
• Enter Layer 3 aggregate interface view: interface route-aggregation interface-number | N/A |
| 3.   | Enable BFD for the aggregation group. | link-aggregation bfd ipv4 source ip-address destination ip-address | By default, BFD is disabled for an aggregation group. The source and destination IP addresses of BFD sessions must be unicast addresses excluding 0.0.0.0. |

**Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection**

⚠️ **CAUTION:**

- Changing reference port selection criteria might cause transient traffic interruption. Make sure you understand the impact of this task on your network.

- You must perform this task at both ends of the aggregate link so the peer aggregation systems use the same criteria for reference port selection.

Perform this task to ensure that a dynamic aggregation group selects a high-speed member port as the reference port.

To configure a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter aggregate interface view. | • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number  
• Enter Layer 3 aggregate interface view: interface route-aggregation interface-number | N/A |
### Shutting down an aggregate interface

Shutting down or bringing up an aggregate interface affects the aggregation states and link states of member ports in the corresponding aggregation group as follows:

- When an aggregate interface is shut down, all Selected ports in the corresponding aggregation group become Unselected ports and all member ports go down.
- When an aggregate interface is brought up, the aggregation states of member ports in the corresponding aggregation group are recalculated.

To shut down an aggregate interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. <strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter aggregate interface view. <strong>interface bridge-aggregation interface-number</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Shut down the aggregate interface or subinterface. <strong>shutdown</strong></td>
</tr>
</tbody>
</table>

### Enabling packet statistics for a Layer 3 aggregate subinterface

**IMPORTANT:**
This feature is supported only in R2612 and later.

The packet statistics feature is CPU intensive. When you use this command for Layer 3 aggregate subinterfaces, make sure you fully understand its impact on system performance.

This feature collects only incoming packet statistics on Layer 3 aggregate subinterfaces.
To enable packet statistics for a Layer 3 aggregate subinterface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 aggregate subinterface view.</td>
<td>interface route-aggregation interface-number.subnumber</td>
</tr>
<tr>
<td>3.</td>
<td>Enable packet statistics for the Layer 3 aggregate subinterface.</td>
<td>traffic-statistic enable</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Display the packet statistics for the Layer 3 aggregate subinterface.</td>
<td>display interface route-aggregation interface-number.subnumber</td>
</tr>
</tbody>
</table>

Restoring the default settings for an aggregate interface

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

To restore the default settings for an aggregate interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
</tbody>
</table>
| 2.   | Enter aggregate interface view. | Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number  
  Enter Layer 3 aggregate interface or subinterface view: interface route-aggregation { interface-number | interface-number.subnumber }  
  Enter S-channel bundle interface view: interface schannel-bundle interface-number |
| 3.   | Restore the default settings for the aggregate interface. | default |

Configuring load sharing for link aggregation groups

This section explains how to configure the 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.

The destination port and source port criteria of the global load sharing mode also take effect on aggregation groups that have group-specific load sharing settings. If the global load sharing mode contains one or both of these criteria, these aggregation groups use both the port load sharing settings and group-specific load sharing settings.
### Setting the global link-aggregation load sharing mode

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>link-aggregation global load-sharing mode { destination-ip</td>
<td>destination-mac</td>
</tr>
</tbody>
</table>

### Setting the group-specific load sharing mode

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number  
• Enter Layer 3 aggregate interface view: interface route-aggregation interface-number | N/A |
| 3.   | link-aggregation load-sharing mode { ( destination-ip | destination-mac | source-ip | source-mac ) * | flexible } | By default, the group-specific load sharing mode is the same as the global load sharing mode. |

### Specifying ignored packet fields for default link-aggregation load sharing

In default load sharing mode, an aggregation group might fail to load share traffic in a balanced manner. To resolve the problem, you can configure the device to ignore specific packet fields for link-aggregation load sharing. The specified packet field values are ignored during the load sharing calculation.

To specify ignored packet fields for default link-aggregation load sharing:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>link-aggregation load-sharing ignore { destination-ip</td>
<td>destination-mac</td>
</tr>
</tbody>
</table>
Enabling local-first load sharing for link aggregation

About local-first load sharing

Use local-first load sharing in a multidevice link aggregation scenario to distribute traffic preferentially across member ports on the ingress 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 14. For more information about IRF, see Virtual Technologies Configuration Guide.

Figure 14 Load sharing for multidevice link aggregation in an IRF fabric

Configuration restrictions and guidelines

On a VXLAN network, you must enable local-first load sharing on the transport-facing interface for a VXLAN tunnel if that interface is one of the following types:

- Layer 3 aggregate interface.
- VLAN interface for a VLAN that contains Layer 2 aggregate interfaces.

For more information about VXLAN, see VXLAN Configuration Guide.

Configuration procedure

To enable local-first load sharing for link aggregation:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable local-first load sharing for link aggregation.</td>
<td>link-aggregation load-sharing mode local-first</td>
</tr>
</tbody>
</table>
Configuring link aggregation load sharing algorithm settings

To optimize traffic distribution on aggregate links, you can configure the link aggregation load sharing algorithm and the hash seed. The algorithm determines the CRC calculation method. The hash seed is a parameter used in hashing.

In default load sharing mode, if the device fails to load share traffic flows across all Selected ports, repeat the following procedure until the problem is resolved:

1. Configure the load sharing algorithm or hash seed. You can specify algorithm 1 to 8 in sequence.
2. Use the `display counters` command to view traffic statistics on Selected ports.

You can use a load sharing algorithm and a hash seed individually or in combination to obtain the optimal load sharing performance.

This feature does not take effect on per-flow load sharing.

To configure a link aggregation load sharing algorithm:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a link aggregation load sharing algorithm.</td>
<td><code>link-aggregation global load-sharing algorithm algorithm-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Configure a link aggregation load sharing hash seed.</td>
<td><code>link-aggregation global load-sharing seed seed-number</code></td>
</tr>
</tbody>
</table>

Setting the global load sharing mode for MAC-in-MAC traffic

Perform this task to set the global load sharing mode for MAC-in-MAC traffic on the aggregate links of a backbone core bridge. For more information about backbone core bridges, see "Configuring PBB."

MAC-in-MAC traffic can be load shared based on any of the following items:

- The outer frame header, and source and destination ports.
- The inner frame header, and source and destination ports.

To set the global load sharing mode for MAC-in-MAC traffic:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the global load sharing mode for MAC-in-MAC traffic.</td>
<td>`link-aggregation global load-sharing minm { inner</td>
</tr>
</tbody>
</table>

Enabling link-aggregation traffic redirection

About link-aggregation traffic redirection

This feature redirects traffic on a Selected port to the remaining available Selected ports of an aggregation group if one of the following events occurs:
The port is shut down by using the `shutdown` command.

The slot that hosts the port reboots, and the aggregation group spans multiple slots.

This feature ensures zero packet loss for known unicast traffic, but does not protect unknown unicast traffic.

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

**Configuration restrictions and guidelines**

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

- Link-aggregation traffic redirection applies only to dynamic link aggregation groups.
- 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 when a slot reboots, do not enable spanning tree together with link-aggregation traffic redirection.
- Link-aggregation traffic redirection does not operate correctly on an edge aggregate interface.
- As a best practice, enable link-aggregation traffic redirection on aggregate interfaces. If you enable this feature globally, communication with a third-party peer device might be affected if the peer is not compatible with this feature.

**Enabling link-aggregation traffic globally**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enable link-aggregation traffic redirection globally.</td>
<td><code>link-aggregation lacp traffic-redirect-notification enable</code></td>
</tr>
</tbody>
</table>

**Enabling link-aggregation traffic redirection for an aggregation group**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter aggregate interface view.</td>
<td><code>interface bridge-aggregation interface-number</code>&lt;br&gt;<code>interface route-aggregation interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable link-aggregation traffic redirection for the aggregation group.</td>
<td><code>link-aggregation lacp traffic-redirect-notification</code></td>
</tr>
</tbody>
</table>
### Specifying link aggregation management VLANs and management port

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify link aggregation management VLANs.</td>
<td>link-aggregation management-vlan vlan-id-list</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the port as a management port for its aggregation group.</td>
<td>link-aggregation management-port</td>
</tr>
</tbody>
</table>

### Excluding a subnet from load sharing on aggregate links

**About excluding subnets from load sharing on aggregate links**

Typically, an aggregate interface distributes traffic across its Selected member ports. The uplink and downlink traffic of a host might be distributed to different member ports, as shown in Figure 15. To make sure the bidirectional traffic of a subnet traverses the same member port, you can exclude that subnet from load sharing by specifying it as a link aggregation management subnet.

When an aggregate interface receives an ARP packet from the management subnet, the device looks up the sender IP address in the ARP table for a matching entry.

- If no matching entry exists, the device creates an ARP entry on the aggregation member port from which the packet came in. This mechanism ensures that the returned downlink traffic will be forwarded out of the member port that received the uplink traffic.
- If an ARP entry already exists on a different port than the aggregate interface or its member ports, the device does not update that ARP entry. Instead, the device broadcasts an ARP request out of all ports to relearn the ARP entry.

When an aggregate interface sends an ARP packet to the management subnet, the device sends the packet out of all Selected member ports of the aggregate interface.

As shown in Figure 15, an aggregate link is established between the server and the IRF fabric. The server sends all uplink traffic of a subnet through Port C1 to Port A1 on the IRF fabric. If that subnet is not specified as a management subnet, the IRF fabric distributes its downlink traffic across Port A1 and Port B2. To send the downlink traffic of that subnet to the server only through Port A1, you can specify the subnet as a link aggregation management subnet.
Configuration restrictions and guidelines

You can configure a maximum of 20 management subnets.

To ensure correct packet forwarding, delete all ARP entries of a subnet before you specify it as a management subnet or after you remove it from the management subnet list.

If you are using link aggregation management subnets, do not use the following features:

- DRNI. For more information, see *Layer 2—LAN Switching Configuration Guide*.
- ARP snooping. For more information, see *Layer 3—IP Services Configuration Guide*.
- MPLS L2VPN. For more information, see *MPLS Configuration Guide*.

Configuration procedure

To exclude a subnet from load sharing on aggregate links:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify a link aggregation management subnet.</td>
<td>link-aggregation management-subnet ip-address { mask</td>
</tr>
</tbody>
</table>

Enabling a Layer 2 aggregate interface to reflect incoming packets back

By default, the device drops a packet if its outgoing interface is the incoming interface where the packet arrived. To have a Layer 2 aggregate interface reflect a packet back when it is both the incoming and outgoing interfaces of that packet, perform this task.

To enable a Layer 2 aggregate interface to reflect incoming packets back:
Enabling transparent LACPDU transmission

About transparent LACPDU transmission

To establish a dynamic aggregation between two remote CEs in a VPLS network, use transparent LACPDU transmission on the PEs to which the CEs attached, as shown in Figure 16. This feature enables the PEs to forward LACPDUs for the CEs to establish a dynamic aggregation. If this feature is disabled, the PEs terminate the LACPDUs. The remote CEs cannot establish dynamic aggregations.

Figure 16 Application scenario of transparent LACPDU transmission

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 aggregate interface view.</td>
<td>interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable port bridging.</td>
<td>port bridge enable</td>
</tr>
</tbody>
</table>

Configuration prerequisites

Perform the following tasks on PEs:

1. Configure the untagged or default frame match criterion for the Ethernet service instances on the interfaces connected to CEs.
2. Map the Ethernet service instances to different VSIs and set the access mode to Ethernet for the VSIs.

For more information about VPLS and Ethernet service instances, see VPLS configuration in MPLS Configuration Guide.

Configuration restrictions and guidelines

When you use this feature on the PEs, follow these guidelines:

- Enable transparent LACPDU transmission on the interfaces that transmit traffic between CEs and PEs and between PEs.
- Do not use an interface for link aggregation if you enable transparent LACPDU transmission on that interface. With transparent LACPDU transmission enabled, an interface cannot be selected for aggregation.

Configuration procedure

To enable transparent LACPDU transmission on an interface:
### Step 1: Enter system view.
- **Command**: `system-view`  
  - **Remarks**: N/A

### Step 2: Enter interface view.
- **Command**: `interface interface-type interface-number`  
  - **Remarks**: N/A

### Step 3: Enable transparent LACPDU transmission.
- **Command**: `lACP transparent enable`  
  - **Remarks**: By default, transparent LACPDU transmission is disabled.

---

## Configuring S-MLAG

### Configuration restrictions and guidelines

This feature is supported only in R2612 and later.

S-MLAG is intended for a non-IRF environment. Do not configure it on an IRF fabric. For more information about IRF, see *Virtual Technologies Configuration Guide*.

An S-MLAG group can contain only one aggregate interface on each device.

The aggregate interfaces in an S-MLAG group cannot be used as DR interfaces or IPPs in DRNI. For more information about DR interfaces and IPPs, see "Configuring DRNI."

Do not configure the following settings on S-MLAG devices:

- LACP MAD.
- Link-aggregation traffic redirection.
- Maximum or minimum number of Selected ports.
- Automatic member port assignment.
- Ignoring port speed in setting the aggregation states of member ports.

As a best practice, maintain consistency across S-MLAG devices in service feature configuration.

### Configuration prerequisites

Configure the link aggregation settings other than S-MLAG settings on each S-MLAG device. Make sure the settings are consistent across the S-MLAG devices.

### Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | `lACP system-mac mac-address` | By default, the LACP system MAC address is the bridge MAC address of the device.  
All S-MLAG devices must use the same LACP system MAC address. |
| 3.   | `lACP system-priority priority` | By default, the LACP system priority is 32768.  
All S-MLAG devices must use the same LACP system priority. |
| 4.   | `lACP system-number number` | By default, the LACP system number is not set.  
You must assign a unique LACP system number to each S-MLAG device. |
Step | Command | Remarks
--- | --- | ---
5. Enter Layer 2 aggregate interface view. | interface bridge-aggregation interface-number | N/A
6. Set the link aggregation mode to dynamic. | link-aggregation mode dynamic | By default, an aggregation group operates in static mode.
7. Assign the aggregate interface to an S-MLAG group. | port s-mlag group group-id | By default, an aggregate interface is not assigned to any S-MLAG group.

Displaying and maintaining Ethernet link aggregation

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information for an aggregate interface or multiple aggregate interfaces.</td>
<td>display interface [ { bridge-aggregation</td>
</tr>
<tr>
<td>Display the local system ID.</td>
<td>display lacp system-id</td>
</tr>
<tr>
<td>Display the global or group-specific link-aggregation load sharing modes.</td>
<td>display link-aggregation load-sharing mode [ interface [ { bridge-aggregation</td>
</tr>
<tr>
<td>Display forwarding information for the specified traffic flow.</td>
<td>display link-aggregation load-sharing path interface { bridge-aggregation</td>
</tr>
<tr>
<td>Display detailed link aggregation information for link aggregation member ports.</td>
<td>display link-aggregation member-port [ interface-list</td>
</tr>
<tr>
<td>Display summary information about all aggregation groups.</td>
<td>display link-aggregation summary</td>
</tr>
<tr>
<td>Display detailed information about the specified aggregation groups.</td>
<td>display link-aggregation verbose [ { bridge-aggregation</td>
</tr>
<tr>
<td>Clear LACP statistics for the specified link aggregation member ports.</td>
<td>reset lacp statistics [ interface interface-list ]</td>
</tr>
<tr>
<td>Clear statistics for the specified aggregate interfaces.</td>
<td>reset counters interface [ { bridge-aggregation</td>
</tr>
</tbody>
</table>
Ethernet link aggregation configuration examples

Layer 2 static aggregation configuration example

Network requirements

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

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

Figure 17 Network diagram

Configuration procedure

1. Configure Device A:

   # Create VLAN 10, and assign port Ten-GigabitEthernet 1/0/4 to VLAN 10.
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] port ten-gigabitethernet 1/0/4
   [DeviceA-vlan10] quit

   # Create VLAN 20, and assign port Ten-GigabitEthernet 1/0/5 to VLAN 20.
   [DeviceA] vlan 20
   [DeviceA-vlan20] port ten-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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to link aggregation group 1.
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 1
   [DeviceA-Ten-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
Port: A -- Auto port, M -- Management port, R -- Reference port
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: NonS
Management VLANs: None

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority</th>
<th>Oper-Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
</tbody>
</table>
```

The output shows that link aggregation group 1 is a Layer 2 static aggregation group that contains three Selected ports.

### Layer 2 dynamic aggregation configuration example

#### Network requirements

On the network shown in Figure 18, perform the following tasks:

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

1. Configure Device A:

   # Create VLAN 10, and assign the port Ten-GigabitEthernet 1/0/4 to VLAN 10.
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] port ten-gigabitethernet 1/0/4
   [DeviceA-vlan10] quit

   # Create VLAN 20, and assign the port Ten-GigabitEthernet 1/0/5 to VLAN 20.
   [DeviceA] vlan 20
   [DeviceA-vlan20] port ten-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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to link aggregation
group 1.
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   [DeviceA] interface ten-gigabitethernet 1/0/3
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 1
   [DeviceA-Ten-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
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: NonS
Management VLANS: None
System ID: 0x8000, 000f-e267-6c6a

Local:
<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1(R)</td>
<td>S</td>
<td>32768</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>S</td>
<td>32768</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>S</td>
<td>32768</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>{ACDEF}</td>
</tr>
</tbody>
</table>

Remote:
<table>
<thead>
<tr>
<th>Actor</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>SystemID</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>32768</td>
<td>81</td>
<td>1 0x8000, 000f-e267-57ad</td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>32768</td>
<td>82</td>
<td>1 0x8000, 000f-e267-57ad</td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>32768</td>
<td>83</td>
<td>1 0x8000, 000f-e267-57ad</td>
<td>{ACDEF}</td>
</tr>
</tbody>
</table>

The output shows that link aggregation group 1 is a Layer 2 dynamic aggregation group that contains three Selected ports.

Layer 2 aggregation load sharing configuration example

Network requirements

On the network shown in Figure 19, perform the following tasks:

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

1. Configure Device A:
   
   # Create VLAN 10, and assign the port Ten-GigabitEthernet 1/0/5 to VLAN 10.
   ```
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] port ten-gigabitethernet 1/0/5
   [DeviceA-vlan10] quit
   ```
   # Create VLAN 20, and assign the port Ten-GigabitEthernet 1/0/6 to VLAN 20.
   ```
   [DeviceA] vlan 20
   [DeviceA-vlan20] port ten-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
   ```
   # Assign ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to link aggregation group 1.
   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-Ten-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 Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to link aggregation group 2.

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

[DeviceA] interface ten-gigabitethernet 1/0/4
[DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 2
[DeviceA-Ten-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
Port: A -- Auto port, M -- Management port, R -- Reference port
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
Management VLANs: None

  Port     Status  Priority Oper-Key
  XGE1/0/1 S       32768    1
  XGE1/0/2 S       32768    1

Aggregate Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None

  Port     Status  Priority Oper-Key
  XGE1/0/3 S       32768    2
  XGE1/0/4 S       32768    2
```

The output shows that:

- Link aggregation groups 1 and 2 are both load-shared Layer 2 static aggregation groups.
- Each aggregation group contains two Selected ports.
# Display all the group-specific load sharing modes on Device A.

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

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

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

The output shows that:
- Link aggregation group 1 load shares packets based on source MAC addresses.
- Link aggregation group 2 load shares packets based on destination MAC addresses.

## Layer 2 edge aggregate interface configuration example

### Network requirements

As shown in Figure 20, a Layer 2 dynamic aggregation group is configured on the device. The server is not configured with dynamic link aggregation.

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

### Figure 20 Network diagram

![Diagram](image)

### Configuration procedure

```
# Create Layer 2 aggregate interface Bridge-Aggregation 1, and set the link aggregation mode to dynamic.
<Device> system-view
[Device] interface bridge-aggregation 1
[Device-Bridge-Aggregation1] link-aggregation mode dynamic

# Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an edge aggregate interface.
[Device-Bridge-Aggregation1] lacp edge-port
[Device-Bridge-Aggregation1] quit

# Assign ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to link aggregation group 1.
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[Device-Ten-GigabitEthernet1/0/1] quit
[Device] interface ten-gigabitethernet 1/0/2
[Device-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[Device-Ten-GigabitEthernet1/0/2] quit
```

### Verifying the configuration

```
# Display detailed information about all aggregation groups on the device when the server is not configured with dynamic link aggregation.
[Device] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
```
The output shows that Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are in Individual state when they do not receive LACPDUs from the server. Both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 can forward traffic. When one port fails, its traffic is automatically switched to the other port.

Layer 3 static aggregation configuration example

Network requirements

On the network shown in Figure 21, perform the following tasks:

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

Figure 21 Network diagram

<table>
<thead>
<tr>
<th>XGE1/0/1</th>
<th>XGE1/0/2</th>
<th>XGE1/0/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device A</td>
<td>Device B</td>
<td></td>
</tr>
</tbody>
</table>

| RAGG1 | 192.168.1.1/24 | RAGG1 | 192.168.1.2/24 |

Configuration procedure

1. Configure Device A:

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

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

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

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   ```
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

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: NonS
Management VLANs: None

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority</th>
<th>Oper-Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
</tbody>
</table>

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

Layer 3 dynamic aggregation configuration example

Network requirements

On the network shown in Figure 22, perform the following tasks:

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

Figure 22 Network diagram

Configuration procedure

1. Configure Device A:
    
    # Create Layer 3 aggregate interface Route-Aggregation 1.
    
    <DeviceA> system-view
[DeviceA] interface route-aggregation 1

# Set the link aggregation mode to dynamic.
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic

# Configure an IP address and subnet mask for Route-Aggregation 1.
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit

# Assign Layer 3 Ethernet interfaces Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to aggregation group 1.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-Ten-GigabitEthernet1/0/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-Ten-GigabitEthernet1/0/3] quit

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

Verifying the configuration

# Display detailed information about all aggregation groups on Device A.
[DeviceA] display link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: NonS
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a

Local:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1(R)</td>
<td>S</td>
<td>32768</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>S</td>
<td>32768</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>S</td>
<td>32768</td>
<td>13</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote:

<table>
<thead>
<tr>
<th>Actor</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>SystemID</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>32768</td>
<td>81</td>
<td>1 0x8000, 000f-e267-57ad</td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>32768</td>
<td>81</td>
<td>1 0x8000, 000f-e267-57ad</td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>32768</td>
<td>81</td>
<td>1 0x8000, 000f-e267-57ad</td>
<td>{ACDEF}</td>
</tr>
</tbody>
</table>

The output shows that link aggregation group 1 is a Layer 3 dynamic aggregation group that contains three Selected ports.
Layer 3 aggregation load sharing configuration example

Network requirements

On the network shown in Figure 23, perform the following tasks:

- Configure Layer 3 static aggregation groups 1 and 2 on Device A and Device B, respectively.
- Configure IP addresses and subnet masks for the corresponding Layer 3 aggregate interfaces.
- Configure link aggregation group 1 to load share packets based on source IP addresses.
- Configure link aggregation group 2 to load share packets based on destination IP addresses.

Figure 23 Network diagram

![Network Diagram]

Configuration procedure

1. Configure Device A:

   # Create Layer 3 aggregate interface Route-Aggregation 1.
   <DeviceA> system-view
   [DeviceA] interface route-aggregation 1

   # Configure Layer 3 aggregation group 1 to load share packets based on source IP addresses.
   [DeviceA-Route-Aggregation1] link-aggregation load-sharing mode source-ip

   # Configure an IP address and subnet mask for Layer 3 aggregate interface Route-Aggregation 1.
   [DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
   [DeviceA-Route-Aggregation1] quit

   # Assign Layer 3 Ethernet interfaces Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 1.
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
   [DeviceA-Ten-GigabitEthernet1/0/2] quit

   # Create Layer 3 aggregate interface Route-Aggregation 2.
   [DeviceA] interface route-aggregation 2

   # Configure Layer 3 aggregation group 2 to load share packets based on destination IP addresses.
   [DeviceA-Route-Aggregation2] link-aggregation load-sharing mode destination-ip

   # Configure an IP address and subnet mask for Layer 3 aggregate interface Route-Aggregation 2.
   [DeviceA-Route-Aggregation2] ip address 192.168.2.1 24
   [DeviceA-Route-Aggregation2] quit

   # Assign Layer 3 Ethernet interfaces Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 2.
   [DeviceA] interface ten-gigabitethernet 1/0/3
Verifying the configuration

# Display detailed information about all aggregation groups on Device A.
[DeviceA] display link-aggregation verbose

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

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority</th>
<th>Oper-Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>S</td>
<td>32768</td>
<td>1</td>
</tr>
</tbody>
</table>

Aggregate Interface: Route-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority</th>
<th>Oper-Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/3</td>
<td>S</td>
<td>32768</td>
<td>2</td>
</tr>
<tr>
<td>XGE1/0/4</td>
<td>S</td>
<td>32768</td>
<td>2</td>
</tr>
</tbody>
</table>

The output shows that:
- Link aggregation groups 1 and 2 are both load-shared Layer 3 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

Route-Aggregation1 Load-Sharing Mode:
source-ip address

Route-Aggregation2 Load-Sharing Mode:
destination-ip address

The output shows that:
- Link aggregation group 1 load shares packets based on source IP addresses.
- Link aggregation group 2 load shares packets based on destination IP addresses.
S-MLAG configuration example

Network requirements

As shown in Figure 24, configure Device B, Device C, and Device D as S-MLAG devices to establish a multichassis aggregate link with Device A.

Figure 24 Network diagram

Configuration procedure

1. Configure Device A:
   # Create Layer 2 aggregate interface Bridge-Aggregation 10, and set the link aggregation mode to dynamic.
   <DeviceA> system-view
   [DeviceA] interface bridge-aggregation 10
   [DeviceA-Bridge-Aggregation10] link-aggregation mode dynamic
   [DeviceA-Bridge-Aggregation10] quit
   # Assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to aggregation group 10.
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 10
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 10
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   [DeviceA] interface ten-gigabitethernet 1/0/3
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 10
   [DeviceA-Ten-GigabitEthernet1/0/3] quit

2. Configure Device B:
   # Set the LACP system MAC address to 0001-0001-0001.
   <DeviceB> system-view
   [DeviceB] lacp system-mac 1-1-1
   # Set the LACP system priority to 123.
   [DeviceB] lacp system-priority 123
   # Set the LACP system number to 1.
   [DeviceB] lacp system-number 1
   # Create Layer 2 aggregate interface Bridge-Aggregation 2, and set the link aggregation mode to dynamic.
3. Configure Device C:
   # Set the LACP system MAC address to 0001-0001-0001.
   <DeviceC> system-view
   [DeviceC] lACP system-mac 1-1-1
   # Set the LACP system priority to 123.
   [DeviceC] lACP system-priority 123
   # Set the LACP system number to 2.
   [DeviceC] lACP system-number 2
   # Create Layer 2 aggregate interface Bridge-Aggregation 3, and set the link aggregation mode
to dynamic.
   [DeviceC] interface bridge-aggregation 3
   [DeviceC-Bridge-Aggregation3] link-aggregation mode dynamic
   # Assign Bridge-Aggregation 3 to S-MLAG group 100.
   [DeviceC-Bridge-Aggregation3] port s-mlag group 100
   # Assign Ten-GigabitEthernet 1/0/1 to aggregation group 3.
   [DeviceC] interface ten-gigabitethernet 1/0/1
   [DeviceC-Ten-GigabitEthernet1/0/1] port link-aggregation group 3
   [DeviceC-Ten-GigabitEthernet1/0/1] quit

4. Configure Device D:
   # Set the LACP system MAC address to 0001-0001-0001.
   <DeviceD> system-view
   [DeviceD] lACP system-mac 1-1-1
   # Set the LACP system priority to 123.
   [DeviceD] lACP system-priority 123
   # Set the LACP system number to 3.
   [DeviceD] lACP system-number 3
   # Create Layer 2 aggregate interface Bridge-Aggregation 4, and set the link aggregation mode
to dynamic.
   [DeviceD] interface bridge-aggregation 4
   [DeviceD-Bridge-Aggregation4] link-aggregation mode dynamic
   # Assign Bridge-Aggregation 4 to S-MLAG group 100.
   [DeviceD-Bridge-Aggregation4] port s-mlag group 100
   # Assign Ten-GigabitEthernet 1/0/1 to aggregation group 4.
   [DeviceD] interface ten-gigabitethernet 1/0/1
   [DeviceD-Ten-GigabitEthernet1/0/1] port link-aggregation group 4
   [DeviceD-Ten-GigabitEthernet1/0/1] quit

Verifying the configuration
   # Verify that Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 on Device A are Selected
   ports.
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 40fa-264f-0100

Local:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1(R)</td>
<td>S</td>
<td>32768</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>S</td>
<td>32768</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>S</td>
<td>32768</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote:

<table>
<thead>
<tr>
<th>Actor</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>SystemID</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>32768</td>
<td>16385</td>
<td>50100 0x7b , 0001-0001-0001</td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>32768</td>
<td>32769</td>
<td>50100 0x7b , 0001-0001-0001</td>
<td>{ACDEF}</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>32768</td>
<td>49153</td>
<td>50100 0x7b , 0001-0001-0001</td>
<td>{ACDEF}</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an isolation group.</td>
<td>port-isolate group group-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The configuration in Layer 2 Ethernet interface view applies only to the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Assign the port to the isolation group.</td>
<td>port-isolate enable group group-id</td>
</tr>
</tbody>
</table>

Displaying and maintaining port isolation

Execute display commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display isolation group information.</td>
<td>display port-isolate group [ group-id ]</td>
</tr>
</tbody>
</table>
Port isolation configuration example

Network requirements

As shown in Figure 25:

- LAN users Host A, Host B, and Host C are connected to Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 1/0/2, and Ten-GigabitEthernet 1/0/3 on the device, respectively.
- The device connects to the Internet through Ten-GigabitEthernet 1/0/4.

Configure the device to provide Internet access for the hosts, and isolate them from one another at Layer 2.

Figure 25 Network diagram

Configuration procedure

# Create isolation group 1.
<Device> system-view
[Device] port-isolate group 1

# Assign Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 1/0/2, and Ten-GigabitEthernet 1/0/3 to isolation group 1.
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port-isolate enable group 1
[Device-Ten-GigabitEthernet1/0/1] quit
[Device] interface ten-gigabitethernet 1/0/2
[Device-Ten-GigabitEthernet1/0/2] port-isolate enable group 1
[Device-Ten-GigabitEthernet1/0/2] quit
[Device] interface ten-gigabitethernet 1/0/3
[Device-Ten-GigabitEthernet1/0/3] port-isolate enable group 1
[Device-Ten-GigabitEthernet1/0/3] quit

Verifying the configuration

# Display information about isolation group 1.
[Device] display port-isolate group 1
Port isolation group information:
  Group ID: 1
  Group members:
    Ten-GigabitEthernet1/0/1   Ten-GigabitEthernet1/0/2   Ten-GigabitEthernet1/0/3

The output shows that Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 1/0/2, and Ten-GigabitEthernet 1/0/3 are assigned to isolation group 1. As a result, Host A, Host B, and Host C are isolated from one another 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 frames

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

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

STP uses two types of BPDUs, configuration BPDUs and topology change notification (TCN) BPDUs.

Configuration BPDUs

Devices exchange configuration BPDUs to elect the root bridge and determine port roles. Figure 26 shows the configuration BPDU format.

Figure 26 Configuration BPDU format

<table>
<thead>
<tr>
<th>DMA</th>
<th>SMA</th>
<th>L/T</th>
<th>LLC header</th>
<th>Payload</th>
</tr>
</thead>
</table>

DMA: Destination MAC address  
SMA: Source MAC address  
L/T: Frame length  
LLC header: Logical link control header  
Payload: BPDU data

<table>
<thead>
<tr>
<th>Fields</th>
<th>Byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol ID</td>
<td>2</td>
</tr>
<tr>
<td>Protocol version ID</td>
<td>1</td>
</tr>
<tr>
<td>BPDU type</td>
<td>1</td>
</tr>
<tr>
<td>Flags</td>
<td>1</td>
</tr>
<tr>
<td>Root ID</td>
<td>8</td>
</tr>
<tr>
<td>Root path cost</td>
<td>4</td>
</tr>
<tr>
<td>Bridge ID</td>
<td>8</td>
</tr>
<tr>
<td>Port ID</td>
<td>2</td>
</tr>
<tr>
<td>Message age</td>
<td>2</td>
</tr>
<tr>
<td>Max age</td>
<td>2</td>
</tr>
<tr>
<td>Hello time</td>
<td>2</td>
</tr>
<tr>
<td>Forward delay</td>
<td>2</td>
</tr>
</tbody>
</table>

The payload of a configuration BPDU includes the following fields:
- **Protocol ID**—Fixed at 0x0000, which represents IEEE 802.1d.
- **Protocol version ID**—Spanning tree protocol version ID. The protocol version ID for STP is 0x00.
- **BPDU type**—Type of the BPDU. The value is 0x00 for a configuration BPDU.
- **Flags**—An 8-bit field indicates the purpose of the BPDU. The lowest bit is the Topology Change (TC) flag. The highest bit is the Topology Change Acknowledge (TCA) flag. All other bits are reserved.
- **Root ID**—Root bridge ID formed by the priority and MAC address of the root bridge.
- **Root path cost**—Cost of the path to the root bridge.
- **Bridge ID**—Designated bridge ID formed by the priority and MAC address of the designated bridge.
- **Port ID**—Designated port ID formed by 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 for STP bridges to transit port state.

Devices use the root bridge ID, root path cost, designated bridge ID, designated port ID, message age, max age, hello time, and forward delay for spanning tree calculation.

**TCN BPDDUs**

Devices use TCN BPDDUs to announce changes in the network topology. Figure 27 shows the TCN BPDU format.

**Figure 27 TCN BPDU format**

<table>
<thead>
<tr>
<th>DMA</th>
<th>SMA</th>
<th>L/T</th>
<th>LLC header</th>
<th>Payload</th>
</tr>
</thead>
</table>

DMA: Destination MAC address  
SMA: Source MAC address  
L/T: Frame length  
LLC header: Logical link control header  
Payload: BPDU data

The payload of a TCN BPDU includes the following fields:
- **Protocol ID**—Fixed at 0x0000, which represents IEEE 802.1d.
- **Protocol version ID**—Spanning tree protocol version ID. The protocol version ID for STP is 0x00.
- **BPDU type**—Type of the BPDU. The value is 0x80 for a TCN BPDU.

A non-root bridge sends TCN BPDDUs when one of the following events occurs on the bridge:
- A port transits to the forwarding state, and the bridge has a minimum of one designated port.
- A port transits from the forwarding or learning state to the blocking state.

The non-root bridge uses TCN BPDDUs to notify the root bridge once the network topology changes. The root bridge then sets the TC flag in its configuration BPDU and propagates it to other bridges.
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

<table>
<thead>
<tr>
<th>Classification</th>
<th>Designated bridge</th>
<th>Designated port</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a device</td>
<td>Device directly connected to the local device and responsible for forwarding BPDUs to the local device.</td>
<td>Port through which the designated bridge forwards BPDUs to this device.</td>
</tr>
<tr>
<td>For a LAN</td>
<td>Device responsible for forwarding BPDUs to this LAN segment.</td>
<td>Port through which the designated bridge forwards BPDUs to this LAN segment.</td>
</tr>
</tbody>
</table>

As shown in Figure 28, Device B and Device C are directly connected to a LAN.

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

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

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

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

Figure 28 Designated bridges and designated ports

Port states

Table 6 lists the port states in STP.
Table 6 STP port states

<table>
<thead>
<tr>
<th>State</th>
<th>Receives/sends BPDUs</th>
<th>Learns MAC addresses</th>
<th>Forwards user data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Listening</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Learning</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Forwarding</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocking</td>
<td>Receive</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Path cost

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

Calculation process of the STP algorithm

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

Calculation process

The STP algorithm uses the following calculation process:

1. Network initialization.
   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. Root bridge selection.
   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.


<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A non-root-bridge device regards the port on which it received the optimum configuration BPDU as the root port. Table 7 describes how the optimum configuration BPDU is selected.</td>
</tr>
</tbody>
</table>
| 2    | Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the other ports.  
• The root bridge ID is replaced with that of the configuration BPDU of the root port.  
• The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost of the root port.  
• The designated bridge ID is replaced with the ID of this device.  
• The designated port ID is replaced with the ID of this port. |
| 3    | The device compares the calculated configuration BPDU with the configuration BPDU on the port whose port role will be determined. Then, the device acts depending on the result of the comparison:  
• If the calculated configuration BPDU is superior, the device performs the following operations:  
  o Considers this port as the designated port. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | - 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. |
| 2    | The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU. |

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

**Table 7 Selecting the optimum configuration BPDU**

<table>
<thead>
<tr>
<th>Step</th>
<th>Actions</th>
</tr>
</thead>
</table>
| 1    | Upon receiving a configuration BPDU on a port, the device compares the priority of the received configuration BPDU with that of the configuration BPDU generated by the port.  
     - If the former priority is lower, the device discards the received configuration BPDU and keeps the configuration BPDU the port generated.  
     - If the former priority is higher, the device replaces the content of the configuration BPDU generated by the port with the content of the received configuration BPDU. |

The following are the principles of configuration BPDU comparison:

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

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

c. If all configuration BPDUs have the same root bridge ID and S value, the following attributes are compared in sequence:
   - Designated bridge IDs.
   - Designated port IDs.
   - IDs of the receiving ports.

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

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

**Example of STP calculation**

*Figure 29* provides an example showing how the STP algorithm works.
As shown in Figure 29, 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 8, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

<table>
<thead>
<tr>
<th>Device</th>
<th>Port name</th>
<th>Configuration BPDU on the port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device A</td>
<td>Port A1</td>
<td>{0, 0, 0, Port A1}</td>
</tr>
<tr>
<td></td>
<td>Port A2</td>
<td>{0, 0, 0, Port A2}</td>
</tr>
<tr>
<td>Device B</td>
<td>Port B1</td>
<td>{1, 0, 1, Port B1}</td>
</tr>
<tr>
<td></td>
<td>Port B2</td>
<td>{1, 0, 1, Port B2}</td>
</tr>
<tr>
<td>Device C</td>
<td>Port C1</td>
<td>{2, 0, 2, Port C1}</td>
</tr>
<tr>
<td></td>
<td>Port C2</td>
<td>{2, 0, 2, Port C2}</td>
</tr>
</tbody>
</table>

2. Configuration BPDUs comparison on each device.

In Table 9, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device A</td>
<td>Port A1 performs the following operations:</td>
<td>• Port A1: {0, 0, 0, Port A1}</td>
</tr>
<tr>
<td></td>
<td>5. Receives the configuration BPDU of Port B1 {1, 0, 1, Port B1}.</td>
<td>• Port A2: {0, 0, 0, Port A2}</td>
</tr>
<tr>
<td></td>
<td>6. Determines that its existing configuration BPDU {0, 0, 0, Port A1} is superior to the received configuration BPDU.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Discards the received one.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port A2 performs the following operations:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Receives the configuration BPDU of Port C1 {2, 0, 2, Port C1}.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Determines that its existing configuration BPDU {0, 0, 0,</td>
<td></td>
</tr>
</tbody>
</table>

102
## Device A

Port A2) is superior to the received configuration BPDU.

10. Discards the received one.

Device A determines that it is both the root bridge and designated bridge in the configuration BPDU 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 BPDU.

### Configuration BPDU on ports after comparison

- Port A: {0, 0, 0, Port A1}
- Port B: {1, 0, 1, Port B1}

## Device B

Port B1 performs the following operations:

11. Receives the configuration BPDU of Port A1 {0, 0, 0, Port A1}.
12. Determines that the received configuration BPDU is superior to its existing configuration BPDU {1, 0, 1, Port B1}.
13. Updates its configuration BPDU.

Port B2 performs the following operations:

14. Receives the configuration BPDU of Port C2 {2, 0, 2, Port C2}.
15. Determines that its existing configuration BPDU {1, 0, 1, Port B2} is superior to the received configuration BPDU.
16. Discards the received BPDU.

Device B performs the following operations:

17. Compares the configuration BPDU of all its ports.
18. Decides that the configuration BPDU of Port B1 is the optimum.
19. Selects Port B1 as the root port with the configuration BPDU unchanged.

Based on the configuration BPDU and path cost of the root port, Device B calculates a designated port configuration BPDU for Port B2 {0, 5, 1, Port B2}. Device B compares it with the existing configuration BPDU of Port B2 {1, 0, 1, Port B2}. Device B determines that the calculated one is superior, and determines that Port B2 is the designated port. It replaces the configuration BPDU on Port B2 with the calculated one, and periodically sends the calculated configuration BPDU.

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device B</td>
<td>Port B1: {0, 0, 0, Port A1}</td>
<td>Port B2: {1, 0, 1, Port B2}</td>
</tr>
</tbody>
</table>

## Device C

Port C1 performs the following operations:

20. Receives the configuration BPDU of Port A2 {0, 0, 0, Port A2}.
21. Determines that the received configuration BPDU is superior to its existing configuration BPDU {2, 0, 2, Port C1}.
22. Updates its configuration BPDU.

Port C2 performs the following operations:

23. Receives the original configuration BPDU of Port B2 {1, 0, 1, Port B2}.
24. Determines that the received configuration BPDU is superior to the existing configuration BPDU {2, 0, 2, Port C2}.
25. Updates its configuration BPDU.

Device C performs the following operations:

26. Compares the configuration BPDU of all its ports.
27. Decides that the configuration BPDU of Port C1 is the optimum.
28. Selects Port C1 as the root port with the configuration BPDU unchanged.

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device C</td>
<td>Port C1: {0, 0, 0, Port A2}</td>
<td>Port C2: {1, 0, 1, Port B2}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device C</td>
<td>Root port (Port C1): {0, 0, 0, Port A2}</td>
<td>Designated port (Port C2): {0, 10, 2, Port C2}</td>
</tr>
</tbody>
</table>
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.

Port C2 performs the following operations:
29. Receives the updated configuration BPDU of Port B2 (0, 5, 1, Port B2).
30. Determines that the received configuration BPDU is superior to its existing configuration BPDU (0, 10, 2, Port C2).
31. Updates its configuration BPDU.

Port C1 performs the following operations:
32. Receives a periodic configuration BPDU (0, 0, 0, Port A2) from Port A2.
33. Determines that it is the same as the existing configuration BPDU.
34. Discards the received BPDU.

Device C determines that the root path cost of Port C1 is larger than that of Port C2. The root path cost of Port C1 is 10, root path cost of the received configuration BPDU (0) plus path cost of Port C1 (10). The root path cost of Port C2 is 9, root path cost of the received configuration BPDU (5) plus path cost of Port C2 (4). Device C determines that the configuration BPDU of Port C2 is the optimum, and selects Port C2 as the root port with the configuration BPDU unchanged.

Based on the configuration BPDU and path cost of the root port, Device C performs the following operations:
35. Calculates a designated port configuration BPDU for Port C1 (0, 9, 2, Port C1).
36. Compares it with the existing configuration BPDU of Port C1 (0, 0, 0, Port A2).
37. Determines that the existing configuration BPDU is superior to the calculated one and blocks Port C1 with the configuration BPDU unchanged.

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.

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
</table>
|          | 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. | Port C1: {0, 0, 0, Port A2}  
Port C2: {0, 5, 1, Port B2} |
|          | Port C2 performs the following operations:  
29. Receives the updated configuration BPDU of Port B2 (0, 5, 1, Port B2).  
30. Determines that the received configuration BPDU is superior to its existing configuration BPDU (0, 10, 2, Port C2).  
31. Updates its configuration BPDU. |                                                                                                           |
|          | Port C1 performs the following operations:  
32. Receives a periodic configuration BPDU (0, 0, 0, Port A2) from Port A2.  
33. Determines that it is the same as the existing configuration BPDU.  
34. Discards the received BPDU. |                                                                                                           |
|          | Device C determines that the root path cost of Port C1 is larger than that of Port C2. The root path cost of Port C1 is 10, root path cost of the received configuration BPDU (0) plus path cost of Port C1 (10). The root path cost of Port C2 is 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. | Port C1: {0, 0, 0, Port A2}  
Port C2: {0, 5, 1, Port B2} |
|          | Based on the configuration BPDU and path cost of the root port, Device C performs the following operations:  
35. Calculates a designated port configuration BPDU for Port C1 (0, 9, 2, Port C1).  
36. Compares it with the existing configuration BPDU of Port C1 (0, 0, 0, Port A2).  
37. Determines that the existing configuration BPDU is superior to the calculated one and blocks Port C1 with the configuration BPDU unchanged. |                                                                                                           |

After the comparison processes described in Table 9, a spanning tree with Device A as the root bridge is established, as shown in Figure 30.
The configuration BPDU forwarding mechanism of STP

The configuration BPDU forwarding mechanism of STP are forwarded according to these guidelines:

- Upon network initiation, every device regards itself as the root bridge and generates configuration BPDU with itself as the root. Then it sends the configuration BPDU at a regular hello interval.

- If the root port receives a configuration BPDU superior to the configuration BPDU of the port, the device performs the following operations:
  - 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 BPDU and the old configuration BPDU will be discarded due to timeout. The device generates a configuration BPDU with itself as the root and sends the BPDU and TCN BPDU. 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. By default, the forward delay is 15 seconds.

  A path failure can cause spanning tree re-calculation 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 must go through the listening and learning states before they transit to the forwarding state. This requires twice the forward delay time and allows the new configuration BPDU to propagate throughout the network.

- Hello time
  The device sends configuration BPDU at the hello time interval to the neighboring devices to ensure that the paths are fault-free. By default, the hello time is 2 seconds. If the device does not receive configuration BPDU within the timeout period, it recalculates the spanning tree.

  The formula for calculating the timeout period is: \[ \text{timeout period} = \text{timeout factor} \times 3 \times \text{hello time}. \]
- 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. By default, the max age is 20 seconds. In the CIST of an MSTP network, the device uses the max age timer to determine whether a configuration BPDU received by a port has expired. If it is expired, a new spanning tree calculation process starts. The max age timer does not take effect on MSTIs.

If a port does not receive any configuration BPDUs within the timeout period, the port transits to the listening state. The device will recalculate the spanning tree. It takes the port 50 seconds to transit back to the forwarding state. This period includes 20 seconds for the max age, 15 seconds for the listening state, and 15 seconds for the learning state.

To ensure a fast topology convergence, make sure the timer settings meet the following formulas:
- \[ 2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age} \]
- \[ \text{Max age} \geq 2 \times (\text{hello time} + 1 \text{ second}) \]

**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.

**RSTP protocol frames**

An RSTP BPDU uses the same format as an STP BPDU except that a Version1 length field is added to the payload of RSTP BPDUs. The differences between an RSTP BPDU and an STP BPDU are as follows:
- **Protocol version ID**—The value is 0x02 for RSTP.
- **BPDU type**—The value is 0x02 for RSTP BPDUs.
- **Flags**—All 8 bits are used.
- **Version1 length**—The value is 0x00, which means no version 1 protocol information is present.

RSTP does not use TCN BPDUs to advertise topology changes. RSTP floods BPDUs with the TC flag set in the network to advertise topology changes.

**Basic concepts in RSTP**

**Port roles**

In addition to root port and designated port, RSTP also uses the following port roles:
- **Alternate port**—Acts as the backup port for a root port. When the root port is blocked, the alternate port takes over.
- **Backup port**—Acts as the backup port of a designated port. When the designated port is invalid, the backup port becomes the new designated port. A loop occurs when two ports of the same spanning tree device are connected, so the device blocks one of the ports. The blocked port is the backup port.
- **Edge port**—Directly connects to a user host rather than a network device or network segment.

**Port states**

RSTP uses the discarding state to replace the disabled, blocking, and listening states in STP. Table 10 shows the differences between the port states in RSTP and STP.
Table 10 Port state differences between RSTP and STP

<table>
<thead>
<tr>
<th>STP port state</th>
<th>RSTP port state</th>
<th>Sends BPDU</th>
<th>Learns MAC addresses</th>
<th>Forwards user data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Discarding</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Blocking</td>
<td>Discarding</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Listening</td>
<td>Discarding</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Learning</td>
<td>Learning</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

How RSTP works

During RSTP calculation, the following events occur:

- If a port in discarding state becomes an alternate port, it retains its state.
- If a port in discarding state is elected as the root port or designated port, it enters the learning state after the forward delay. The port learns MAC addresses, and enters the forwarding state after another forward delay.
  - A newly elected RSTP root port rapidly enters the forwarding state if the following requirements are met:
    - 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 one of the following requirements is met:
    - The designated port is configured as an edge port which directly connects to a user terminal.
    - The designated port connects to a point-to-point link and receives a handshake response from the directly connected device.

RSTP BPDU processing

In RSTP, a non-root bridge actively sends RSTP BPDUs at the hello time through designated ports without waiting for the root bridge to send RSTP BPDUs. This enables RSTP to quickly detect link failures. If a device fails to receive any RSTP BPDUs on a port within triple the hello time, the device considers that a link failure has occurred. After the stored configuration BPDU expires, the device floods RSTP BPDUs with the TC flag set to initiate a new RSTP calculation.

In RSTP, a port in blocking state can immediately respond to an RSTP BPDU with a lower priority than its own BPDU.

As shown in Figure 31, Device A is the root bridge. The priority of Device B is higher than the priority of Device C. Port C2 on Device C is blocked.

When the link between Device A and Device B fails, the following events occur:

1. Device B sends an RSTP BPDU with itself as the root bridge to Device C.
2. Device C compares the RSTP BPDU with its own BPDU.
3. Because the RSTP BPDU from Device B has a lower priority, Device C sends its own BPDU to Device B.
4. Device B considers that Port B2 is the root port and stops sending RSTP BPDUs to Device C.
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 usage of links and bandwidth. Because each VLAN runs 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.

PVST protocol frames

As shown in Figure 32, a PVST BPDU uses the same format as an RSTP BPDU except the following differences:

- The destination MAC address of a PVST BPDU is 01-00-0c-cc-cc-cd, which is a private MAC address.
- Each PVST BPDU carries a VLAN tag. The VLAN tag identifies the VLAN to which the PVST BPDU belongs.
- The organization code and PID fields are added to the LLC header of the PVST BPDU.

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

- An access port sends RSTP BPDUs.
- A trunk or hybrid port sends RSTP BPDUs in the default VLAN and sends PVST BPDUs in other VLANs.
Basic concepts in PVST

PVST uses the same port roles and port states as RSTP for fast convergence. For more information, see "Basic concepts in RSTP."

How PVST works

In PVST, each VLAN runs RSTP independently to maintain its own spanning tree without affecting the spanning trees of other VLANs. In this way, loops in each VLAN are eliminated and traffic of different VLANs is load shared over links. PVST uses RSTP BPDUs in the default VLAN and PVST BPDUs in other VLANs for spanning tree calculation. Hewlett Packard Enterprise PVST implements per-VLAN spanning tree calculation by mapping each VLAN to an MSTI.

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 frames 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 frames 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 protocol frames

Figure 33 shows the format of an MSTP BPDU.
The first 13 fields of an MSTP BPDU are the same as an RSTP BPDU. The other six fields are unique to MSTP.

- **Protocol version ID**—The value is 0x03 for MSTP.
- **BPDU type**—The value is 0x02 for RSTP/MSTP BPDUs.
- **Root ID**—ID of the common root bridge.
- **Root path cost**—CIST external path cost.
- **Bridge ID**—ID of the regional root for the IST or an MSTI.
- **Port ID**—ID of the designated port in the CIST.
- **Version3 length**—Length of the MSTP-specific fields. Devices use this field for verification upon receiving an MSTP BPDU.
- **MST configuration ID**—Includes the format selector, configuration name, revision level, and configuration digest. The value for format selector is fixed at 0x00. The other parameters are used to identify the MST region for the originating bridge.
- **CIST IRPC**—Internal root path cost (IRPC) from the originating bridge to the root of the MST region.
- **CIST bridge ID**—ID of the bridge that sends the MSTP BPDU.
- **CIST remaining ID**—Remaining hop count. This field limits the scale of the MST region. The regional root sends a BPDU with the remaining hop count set to the maximum value. Each device that receives the BPDU decrements the hop count by one. When the hop count reaches zero, the BPDU is discarded. Devices beyond the maximum hops of the MST region cannot participate in spanning tree calculation. The default remaining hop count is 20.
- **MSTI configuration messages**—Contains MSTI configuration messages. Each MSTI configuration message is 16 bytes. This field can contain 0 to 64 MSTI configuration messages. The number of the MSTI configuration messages is determined by the number of MSTIs in the MST region.
MSTP basic concepts

Figure 34 shows a switched network that contains four MST regions, each MST region containing four MSTP devices. Figure 35 shows the networking topology of MST region 3.

Figure 34 Basic concepts in MSTP

MST region 1

VLAN 1 → MSTI 1
VLAN 2 → MSTI 2
Other VLANs → MSTI 0

MST region 2

MST region 3

VLAN 1 → MSTI 1
VLAN 2 → MSTI 2
Other VLANs → MSTI 0

MST region 4

VLAN 1 → MSTI 1
VLAN 2 → MSTI 2
Other VLANs → MSTI 0

CST

Figure 35 Network diagram and topology of MST region 3

To MST region 4

Device A

MST region 3

Device B

To MST region 2

Device C

Device D

VLAN 1 → MSTI 1
VLAN 2&3 → MSTI 2
Other VLANs → MSTI 0

Top of MSTIs in MST region 3

Regional root

MSTI

A

B

MSTI 1

C

D

A

B

MSTI 2

C

D

MSTI 0
MST region

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

- A spanning tree protocol enabled
- Same region name
- Same VLAN-to-instance mapping configuration
- Same MSTP revision level
- Physically linked together

Multiple MST regions can exist in a switched network. You can assign multiple devices to the same MST region, as shown in Figure 34.

- The switched network contains 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 35, MST region 3 contains 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 35, 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 34 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 34, 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 34, the ISTs (MSTI 0) in all MST regions plus the inter-region CST constitute the CIST of the entire network.

Regional root

The root bridge of the IST or an MSTI within an MST region is the regional root of the IST or MSTI. Based on the topology, different spanning trees in an MST region might have different regional roots, as shown in MST region 3 in Figure 35.
• 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 34, 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 36, an MST region contains 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 36 Port roles

MSTP calculation involves the following port roles:

• **Root port**—Forwards data for a non-root bridge to the root bridge. The root bridge does not have any root port.

• **Designated port**—Forwards data to the downstream network segment or device.

• **Alternate port**—Acts as the backup port for a root port or master port. When the root port or master port is blocked, the alternate port takes over.

• **Backup port**—Acts as the backup port of a designated port. When the designated port is invalid, the backup port becomes the new designated port. A loop occurs when two ports of the same spanning tree device are connected, so the device blocks one of the ports. The blocked port acts as the backup.

• **Edge port**—Directly connects to a user host rather than a network device or network segment.

• **Master port**—Acts as a port on the shortest path from the local MST region to the common root bridge. The master port is not always located on the regional root. It is a root port on the IST or CIST and still a master port on the other MSTIs.

• **Boundary port**—Connects an MST region to another MST region or to an STP/RSTP-running device. In MSTP calculation, a boundary port’s role on an MSTI is consistent with its role on the
CIST. However, that is not true with master ports. A master port on MSTIs is a root port on the CIST.

Port states

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

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

**NOTE:**
When in different MSTIs, a port can be in different states.

A port state is not exclusively associated with a port role. Table 11 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>
<thead>
<tr>
<th>Port role (right) Port state (below)</th>
<th>Root port/master port</th>
<th>Designated port</th>
<th>Alternate port</th>
<th>Backup port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding</td>
<td>√</td>
<td>√</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Learning</td>
<td>√</td>
<td>√</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Discarding</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

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 frame is forwarded along the following paths:
• Within an MST region, the frame is forwarded along the corresponding MSTI.
• Between two MST regions, the frame 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 frames.

In addition to basic MSTP features, the following features 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

Rapid transition mechanism

In STP, a port must wait twice the forward delay (30 seconds by default) before it transits from the blocking state to the forwarding state. The forward delay is related to the hello time and network diameter. If the forward delay is too short, loops might occur. This affects the stability of the network.

RSTP, PVST, and MSTP all use the rapid transition mechanism to speed up port state transition for edge ports, root ports, and designated ports. The rapid transition mechanism for designated ports is also known as the proposal/agreement (P/A) transition.

Edge port rapid transition

As shown in Figure 37, Port C3 is an edge port connected to a host. When a network topology change occurs, the port can immediately transit from the blocking state to the forwarding state because no loop will be caused.

Because a device cannot determine whether a port is directly connected to a terminal, you must manually configure the port as an edge port.

Figure 37 Edge port rapid transition
Root port rapid transition

When a root port is blocked, the bridge will elect the alternate port with the highest priority as the new root port. If the new root port’s peer is in the forwarding state, the new root port immediately transits to the forwarding state.

As shown in Figure 38, Port C2 on Device C is a root port and Port C1 is an alternate port. When Port C2 transits to the blocking state, Port C1 is elected as the root port and immediately transits to the forwarding state.

Figure 38 Root port rapid transition

P/A transition

The P/A transition enables a designated port to rapidly transit to the forwarding state after a handshake with its peer. The P/A transition applies only to point-to-point links.

- P/A transition for RSTP and PVST.

In RSTP or PVST, the ports on a new link or recovered link are designated ports in blocking state. When one of the designated ports transits to the discarding or learning state, it sets the proposal flag in its BPDU. Its peer bridge receives the BPDU and determines whether the receiving port is the root port. If it is the root port, the bridge blocks the other ports except edge ports. The bridge then replies an agreement BPDU to the designated port. The designated port immediately transits to the forwarding state upon receiving the agreement BPDU. If the designated port does not receive the agreement BPDU, it waits for twice the forward delay to transit to the forwarding state.

As shown in Figure 39, the P/A transition operates as follows:

a. Device A sends a proposal BPDU to Device B through Port A1.
b. Device B receives the proposal BPDU on Port B2. Port B2 is elected as the root port.
c. Device B blocks its designated port Port B1 and alternate port Port B3 to eliminate loops.
d. The root port Port B2 transits to the forwarding state and sends an agreement BPDU to Device A.
e. The designated port Port A1 on Device A immediately transits to the forwarding state after receiving the agreement BPDU.
• **P/A transition for MSTP.**

In MSTP, an upstream bridge sets both the proposal and agreement flags in its BPDU. If a downstream bridge receives the BPDU and its receiving port is elected as the root port, the bridge blocks all the other ports except edge ports. The downstream bridge then replies an agreement BPDU to the upstream bridge. The upstream port immediately transits to the forwarding state upon receiving the agreement BPDU. If the upstream port does not receive the agreement BPDU, it waits for twice the forward delay to transit to the forwarding state.

As shown in Figure 40, the P/A transition operates as follows:

a. Device A sets the proposal and agreement flags in its BPDU and sends it to Device B through Port A1.
b. Device B receives the BPDU. Port B1 of Device B is elected as the root port.
c. Device B then blocks all its ports except the edge ports.
d. The root port Port B1 of Device B transits to the forwarding state and sends an agreement BPDU to Device A.
e. Port A1 of Device A immediately transits to the forwarding state upon receiving the agreement BPDU.

### 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:

- When the spanning tree protocol is enabled for a DR system, make sure the DR member devices have the same spanning tree configuration, including:
  - Global spanning tree configuration.
  - Spanning tree configuration on the IPP.
  - Spanning tree configuration on DR interfaces.

Violation of this rule might cause network flapping. IPPs in the DR system do not participate in spanning tree calculation. To view the spanning tree information of DR interfaces, use related display commands on the primary DR device. For more information about the DR system, DR interfaces, and IPPs, see "Configuring DRNI."

- 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."

- To connect a spanning tree network to a TRILL network, make sure the following requirements are met:
  - The spanning tree protocol is disabled on TRILL ports.
  - An edge port is used to connect the spanning tree network to the TRILL network. The edge port can quickly transit to the forwarding state. This prevents network topology changes from influencing the TRILL network.

For more information about TRILL, see TRILL Configuration Guide.

- The spanning tree configurations are mutually exclusive with any of the following features on a port: service loopback group, RRPP, L2PT, and Smart Link.

- Configurations made in system view take effect globally. Configurations made in Ethernet interface view take effect only on the interface. 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

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the root bridge:</td>
</tr>
<tr>
<td>• (Required.) Setting the spanning tree mode</td>
</tr>
<tr>
<td>• (Optional.) Configuring the root bridge or a secondary root bridge</td>
</tr>
<tr>
<td>• (Optional.) Configuring the device priority</td>
</tr>
</tbody>
</table>
### Tasks at a glance

<table>
<thead>
<tr>
<th>Required/Optional</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.)</td>
<td>Configuring the spanning tree feature</td>
</tr>
<tr>
<td>Optional.</td>
<td>Configuring the network diameter of a switched network</td>
</tr>
<tr>
<td>Optional.</td>
<td>Setting spanning tree timers</td>
</tr>
<tr>
<td>Optional.</td>
<td>Setting the timeout factor</td>
</tr>
<tr>
<td>Optional.</td>
<td>Configuring the BPDU transmission rate</td>
</tr>
<tr>
<td>Optional.</td>
<td>Enabling outputting port state transition information</td>
</tr>
</tbody>
</table>

#### Configuring the root bridge:
- (Required.) Setting the spanning tree mode
- Optional. Configuring the root bridge or a secondary root bridge
- Optional. Configuring the device priority
- Optional. Configuring the network diameter of a switched network
- Optional. 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:
- (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 link type
- Optional. Configuring the port priority
- (Optional.) Enabling outputting port state transition information

### RSTP configuration task list

#### Tasks at a glance

<table>
<thead>
<tr>
<th>Required/Optional</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required.</td>
<td>Configuring the spanning tree feature</td>
</tr>
</tbody>
</table>

#### Configuring the root bridge:
- (Required.) Setting the spanning tree mode
- Optional. Configuring the root bridge or a secondary root bridge
- Optional. Configuring the device priority
- Optional. Configuring the network diameter of a switched network
- Optional. 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:
- (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 link type
- Optional. Configuring the port priority
- (Optional.) Enabling outputting port state transition information
### PVST configuration task list

#### Tasks at a glance

**Configuring the root bridge:**
- *(Required.)* Setting the spanning tree mode
- *(Optional.)* Configuring the root bridge or a secondary root bridge
- *(Optional.)* Configuring the device priority
- *(Optional.)* Configuring the network diameter of a switched network
- *(Optional.)* 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:**
- *(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.)* Disabling inconsistent PVID protection

*(Optional.)* Configuring protection features

*(Optional.)* Enabling the device to log events of detecting or receiving TC BPDUs

*(Optional.)* Disabling the device to reactivate the shutdown edge ports

*(Optional.)* Enabling BPDU transparent transmission on a port

*(Optional.)* Enabling SNMP notifications for new-root election and topology change events
MSTP configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the root bridge:</td>
</tr>
<tr>
<td>• (Required.) Setting the spanning tree mode</td>
</tr>
<tr>
<td>• (Required.) Configuring an MST region</td>
</tr>
<tr>
<td>• (Optional.) Configuring the root bridge or a secondary root bridge</td>
</tr>
<tr>
<td>• (Optional.) Configuring the device priority</td>
</tr>
<tr>
<td>• (Optional.) Configuring the maximum hops of an MST region</td>
</tr>
<tr>
<td>• (Optional.) Configuring the network diameter of a switched network</td>
</tr>
<tr>
<td>• (Optional.) Setting spanning tree timers</td>
</tr>
<tr>
<td>• (Optional.) Setting the timeout factor</td>
</tr>
<tr>
<td>• (Optional.) Configuring the BPDU transmission rate</td>
</tr>
<tr>
<td>• (Optional.) Configuring edge ports</td>
</tr>
<tr>
<td>• (Optional.) Configuring the port link type</td>
</tr>
<tr>
<td>• (Optional.) Configuring the mode a port uses to recognize and send MSTP frames</td>
</tr>
<tr>
<td>• (Optional.) Enabling outputting port state transition information</td>
</tr>
<tr>
<td>• (Required.) Enabling the spanning tree feature</td>
</tr>
</tbody>
</table>

| Configuring the leaf nodes: |
| • (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 frames |
| • (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 features |
| (Optional.) Disabling the device to reactivate the shutdown edge ports |
| (Optional.) Enabling BPDU transparent transmission on a port |
| (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.

• **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 PVST-enabled VLANs supported by the device is 144.

• **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.

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 the default VLAN.

To set the spanning tree mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the spanning tree mode.</td>
<td>stp mode (mstp</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter MST region view.</td>
<td>stp region-configuration</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the MST region name.</td>
<td>region-name name</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the VLAN-to-instance mapping table.</td>
<td>• instance instance-id vlan vlan-id-list&lt;br&gt;• vlan-mapping modulo modulo</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the MSTP revision level of the MST region.</td>
<td>revision-level level</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Display the MST region configurations that are not activated yet.</td>
<td>check region-configuration</td>
</tr>
<tr>
<td>7.</td>
<td>Manually activate MST region configuration.</td>
<td>active region-configuration</td>
</tr>
</tbody>
</table>

### 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 a 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 selected.

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

- If you specify only one secondary root bridge, 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 a device as the root bridge by setting the device priority to 0. For the device priority configuration, see "Configuring the device priority."

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the device as the root bridge.</td>
<td>• In STP/RSTP mode: stp root primary&lt;br&gt;• In PVST mode: stp vlan vlan-id-list root primary</td>
</tr>
</tbody>
</table>
### Configuring the device as a secondary root bridge of a specific spanning tree

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the device as a secondary root bridge.</td>
<td></td>
</tr>
</tbody>
</table>

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`

### 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 the device in a specified MSTI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the priority of the device.</td>
<td></td>
</tr>
</tbody>
</table>

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`

### 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, set 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure the maximum hops of the MST region.</td>
<td>stp max-hops hops</td>
<td>The default setting is 20.</td>
</tr>
</tbody>
</table>

**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:

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

**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. This ensures that 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 does not receive 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 whether a configuration BPDU received by a port has expired. If it is expired, a new spanning tree calculation process starts. The max age timer does not take effect on MSTIs.

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

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

As a best practice, specify the network diameter and letting spanning tree protocols automatically calculate the timers based on the network diameter instead of manually setting the spanning tree timers. 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**

When you set spanning tree timers, follow these restrictions and guidelines:

- The length of the forward delay is related to the network diameter of the switched network. The larger the network diameter is, the longer the forward delay time should be. As a best practice, use the automatically calculated value because inappropriate forward delay setting might cause temporary redundant paths or increase the network convergence time.

- 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the forward delay timer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In STP/RSTP/MSTP mode:</td>
<td>stp timer forward-delay time</td>
</tr>
<tr>
<td></td>
<td>• In PVST mode:</td>
<td>stp vlan vlan-id-list timer forward-delay time</td>
</tr>
<tr>
<td>3.</td>
<td>Set the hello timer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In STP/RSTP/MSTP mode:</td>
<td>stp timer hello time</td>
</tr>
<tr>
<td></td>
<td>• In PVST mode:</td>
<td>stp vlan vlan-id-list timer hello time</td>
</tr>
</tbody>
</table>
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.

As a best practice, set the timeout factor to 5, 6, or 7 in the following situations:

- To prevent undesired spanning tree calculations. An upstream device might be too busy to forward configuration BPDUs in time, for example, many Layer 2 interfaces are configured on the upstream device. In this case, the downstream device fails to receive a BPDU within the timeout period and then starts an undesired spanning tree calculation.
- To save network resources on a stable network.

To set the timeout factor:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the timeout factor of the device.</td>
<td>stp timer-factor factor</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the BPDU transmission rate of the ports.</td>
<td>stp transmit-limit limit</td>
</tr>
</tbody>
</table>
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 blocking state to the forwarding state.

Configuration restrictions and guidelines

When you configure edge ports, follow these restrictions and guidelines:

- If BPDU guard is disabled on a port configured as an edge port, the 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 feature and the edge port setting are mutually exclusive.

Configuration procedure

To configure a port as an edge port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the port as an edge port.</td>
<td>stp edged-port</td>
</tr>
</tbody>
</table>

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). The 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 aggregate interface with a speed exceeding 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify a standard for the device to use when it calculates the default path costs of its ports.</td>
<td>stp pathcost-standard { dot1d-1998</td>
</tr>
</tbody>
</table>

### Table 12 Mappings between the link speed and the path cost

<table>
<thead>
<tr>
<th>Link speed</th>
<th>Port type</th>
<th>Path cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>IEEE 802.1d-1998</td>
</tr>
<tr>
<td>0</td>
<td>N/A</td>
<td>65535</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>Single port</td>
<td>1000000</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>100000</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>666666</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing four Selected ports</td>
<td>500000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>Single port</td>
<td>2000000</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>100000</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>66666</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing four Selected ports</td>
<td>50000</td>
</tr>
<tr>
<td>Link speed</td>
<td>Port type</td>
<td>Path cost</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>Single port</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing four Selected ports</td>
<td>4</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>Single port</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing four Selected ports</td>
<td>2</td>
</tr>
<tr>
<td>20 Gbps</td>
<td>Single port</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing four Selected ports</td>
<td>1</td>
</tr>
<tr>
<td>40 Gbps</td>
<td>Single port</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing four Selected ports</td>
<td>1</td>
</tr>
<tr>
<td>100 Gbps</td>
<td>Single port</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing two Selected ports</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Aggregate interface containing three Selected ports</td>
<td>1</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface &lt;interface-type&gt; &lt;interface-number&gt;</td>
</tr>
</tbody>
</table>
| 3.   | Configure the path cost of the ports. | • In STP/RSTP mode: `stp cost <cost-value>`  
• In PVST mode: `stp vlan <vlan-id-list> cost <cost-value>`  
• In MSTP mode: `stp [instance <instance-list>] cost <cost-value>` | 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 Ten-GigabitEthernet 1/0/3 to 200 on MSTI 2.

```plaintext
<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-Ten-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 Ten-GigabitEthernet 1/0/3 to 2000 on VLAN 20 through VLAN 30.

```plaintext
<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-Ten-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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.     | Configure the port priority.                                            | • In STP/RSTP mode: stp port priority priority  
|        |                                                                         | • In PVST mode: stp vlan vlan-id-list port priority priority  
|        |                                                                         | • In MSTP mode: stp [ instance instance-list ] port priority priority |

The default setting is 128 for all ports.

Configuring the port link type

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

Configuration restrictions and guidelines

When you configure the port link type, follow these restrictions and guidelines:

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

Configuration procedure

To configure the link type of a port:
### Configuring the mode a port uses to recognize and send MSTP frames

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td><strong>interface interface-type interface-number</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the mode that the port uses to recognize/send MSTP frames.</td>
<td>**stp compliance { auto</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
</tbody>
</table>
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.

To exclude specific ports from spanning tree calculation and save CPU resources, disable the spanning tree feature for these ports with the `undo stp enable` command. 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enable the spanning tree feature.</td>
<td><code>stp global enable</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Enable the spanning tree feature for the port.</td>
<td><code>stp enable</code></td>
</tr>
</tbody>
</table>

### Enabling the spanning tree feature in PVST mode

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enable the spanning tree feature.</td>
<td><code>stp global enable</code></td>
</tr>
</tbody>
</table>
Performing mCheck

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

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

- The peer STP device is shut down or removed.
- The port cannot detect the change.

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

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

Configuration restrictions and guidelines

When you configure mCheck, follow these restrictions and guidelines:

- The mCheck operation takes effect on devices operating in MSTP, PVST, or RSTP mode.
- When you enable or disable TRILL on a port, the port might send TCN BPDUs to the peer port, which causes the peer port to transit to STP mode. When you disable TRILL and enable STP on a port, As a best practice, perform mCheck on both the port and the peer port.

Performing mCheck globally
Performing mCheck in interface view

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
</tr>
<tr>
<td>3.</td>
<td>Perform mCheck.</td>
</tr>
</tbody>
</table>

Disabling inconsistent PVID protection

In PVST, if two connected ports use different PVIDs, PVST calculation errors might occur. By default, inconsistent PVID protection is enabled to avoid PVST calculation errors. If PVID inconsistency is detected on a port, the system blocks the port.

If different PVIDs are required on two connected ports, disable inconsistent PVID protection on the devices that host the ports. To avoid PVST calculation errors, make sure the following requirements are met:

- Make sure the VLANs on one device do not use the same ID as the PVID of its peer port (except the default VLAN) on another device.
- If the local port or its peer is a hybrid port, do not configure the local and peer ports as untagged members of the same VLAN.
- Disable inconsistent PVID protection on both the local device and the peer device.

This feature takes effect only when the device is operating in PVST mode.

To disable the inconsistent PVID protection feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable the inconsistent PVID protection feature.</td>
<td>stp ignore-pvid-inconsistency</td>
</tr>
</tbody>
</table>

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 BPDUs. 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 enable the spanning tree feature. To avoid traffic interruption, do not configure Digest Snooping when the network is already working well.

Configuration procedure

Use this feature on when your HPE device is connected to a third-party device that uses its private key to calculate the configuration digest.

To configure Digest Snooping:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable Digest Snooping on the interface.</td>
<td>stp config-digest-snooping</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enable Digest Snooping globally.</td>
<td>stp global config-digest-snooping</td>
</tr>
</tbody>
</table>

Digest Snooping configuration example

Network requirements

As shown in Figure 41, 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 41 Network diagram**

![Network Diagram](image)

**Configuration procedure**

# Enable Digest Snooping on Ten-GigabitEthernet 1/0/1 of Device A and enable global Digest Snooping on Device A.

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] stp global config-digest-snooping
```

# Enable Digest Snooping on Ten-GigabitEthernet 1/0/1 of Device B and enable global Digest Snooping on Device B.

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-Ten-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 whether or not an agreement packet from the upstream device is received.
If the upstream device is a third-party device, the rapid state transition implementation might be limited as follows:

- The upstream device uses a rapid transition mechanism similar to that of RSTP.
- The downstream device runs 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 from the upstream device.
2. It sends no agreement 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.

To enable the designated port of the upstream device to transit its state rapidly, enable No Agreement Check on the downstream device's port.

**Configuration prerequisites**

Before you configure the No Agreement Check feature, 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable No Agreement Check.</td>
<td>stp no-agreement-check</td>
</tr>
</tbody>
</table>

No Agreement Check configuration example

Network requirements

As shown in Figure 44, 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 44 Network diagram

Configuration procedure

# Enable No Agreement Check on Ten-GigabitEthernet 1/0/1 of Device A.

<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/1
DeviceA-Ten-GigabitEthernet1/0/1] stp no-agreement-check

Configuring TC Snooping

As shown in Figure 45, an IRF fabric connects to two user networks through double links.

- Device A and Device B form the IRF fabric.
- The spanning tree feature is disabled on Device A and Device B and enabled on all devices in user network 1 and user network 2.
- The IRF fabric transparently transmits BPDUs for both user networks and is not involved in the calculation of spanning trees.

When the network topology changes, it takes time for the IRF fabric to update its MAC address table and ARP table. During this period, traffic in the network might be interrupted.
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.
- The priority of L2PT is higher than that of TC Snooping. When L2PT is enabled on a port, the TC Snooping feature does not take effect on the port.
- TC Snooping does not support the PVST mode.

Configuration procedure

To enable TC Snooping:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Globally disable the spanning tree feature.</td>
<td>When the device starts up with initial settings, the spanning tree feature is globally disabled. When the device starts up with factory defaults, the spanning tree feature is globally enabled. For more information about the initial settings and factory defaults, see Fundamentals Configuration Guide.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable TC Snooping.</td>
<td>By default, TC Snooping is disabled.</td>
</tr>
</tbody>
</table>
Configuring protection features

A spanning tree device supports the following protection features:

- BPDU guard
- Root guard
- Loop guard
- Port role restriction
- TC-BPDU transmission restriction
- TC-BPDU guard
- BPDU drop
- PVST BPDU guard
- Dispute guard

Configuring 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 feature 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 operations:

- 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.

You can configure the BPDU guard feature globally or on a per-edge port basis.

BPDU guard does not take effect on loopback-testing-enabled ports. For more information about loopback testing, see Interface Configuration Guide.

Enabling BPDU guard globally

The global BPDU guard setting takes effect on all edge ports that are not configured by using the stp port bpdu-protection command.

To enable BPDU guard globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable BPDU guard globally.</td>
<td>stp bpdu-protection</td>
</tr>
</tbody>
</table>

Configuring BPDU guard on an interface

An edge port preferentially uses the port-specific BPDU guard setting. If the port-specific BPDU guard setting is not available, the edge port uses the global BPDU guard setting.

To configure BPDU guard on an interface:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure BPDU guard.</td>
<td>stp port bpdu-protection { enable</td>
</tr>
</tbody>
</table>

### 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 feature. 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 operations:

- 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 to 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 feature and the root guard feature are mutually exclusive.

Configure root guard on a designated port.

To enable root guard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the root guard feature.</td>
<td>stp root-protection</td>
</tr>
</tbody>
</table>

### 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 situation, 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 feature 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 feature is mutually exclusive with the root guard feature or the edge port setting.

Configure loop guard on the root port and alternate ports of a device.

To enable loop guard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><strong>system-view</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td><strong>interface</strong> <em>interface-type</em> <em>interface-number</em></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable the loop guard feature for the ports.</td>
<td><strong>stp loop-protection</strong></td>
<td>By default, loop guard is disabled.</td>
</tr>
</tbody>
</table>

### 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 bridge ID change 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><strong>system-view</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td><strong>interface</strong> <em>interface-type</em> <em>interface-number</em></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable port role restriction.</td>
<td><strong>stp role-restriction</strong></td>
<td>By default, port role restriction is disabled.</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>enter system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>interface interface-type</code></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>stp tc-restriction</code></td>
<td>By default, TC-BPDU transmission restriction is disabled.</td>
</tr>
</tbody>
</table>

### 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-BPDU to attack the device, the device will receive a large number of TC-BPDUs within a short time. Then, the device is 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>enter system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>stp tc-protection</code></td>
<td>By default, TC-BPDU guard is enabled.</td>
</tr>
<tr>
<td></td>
<td><code>interface interface-type</code></td>
<td>As a best practice, do not disable this feature.</td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>stp tc-protection threshold</code></td>
<td>The default setting is 6.</td>
</tr>
<tr>
<td></td>
<td><code>number</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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:
### Enabling PVST BPDU guard

An MSTP-enabled device forwards PVST BPDUs as data traffic because it cannot recognize PVST BPDUs. If a PVST-enabled device in another independent network receives the PVST BPDUs, a PVST calculation error might occur. To avoid PVST calculation errors, enable PVST BPDU guard on the MSTP-enabled device. The device shuts down a port if the port receives PVST BPDUs.

To enable PVST BPDU guard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BPDU drop on the interface</td>
<td>bpdu-drop any</td>
</tr>
</tbody>
</table>

### Disabling dispute guard

Dispute guard can be triggered by unidirectional link failures. If an upstream port receives inferior BPDUs from a downstream designated port in forwarding or learning state because of a unidirectional link failure, a loop appears. Dispute guard blocks the upstream designated port to prevent the loop.

As shown in Figure 46, in normal conditions, the spanning tree calculation result is as follows:

- Device A is the root bridge, and Port A1 is a designated port.
- Port B1 is blocked.

When the link between Port A1 and Port B1 fails in the direction of Port A1 to Port B1 and becomes unidirectional, the following events occur:

1. Port A1 can only receive BPDUs and cannot send BPDUs to Port B1.
2. Port B1 does not receive BPDUs from Port A1 for a certain period of time.
3. Device B determines itself as the root bridge.
4. Port B1 sends its BPDUs to Port A1.
5. Port A1 determines the received BPDUs are inferior to its own BPDUs. A dispute is detected.
6. Dispute guard is triggered and blocks Port A1 to prevent a loop.
However, dispute guard might disrupt the network connectivity. You can disable dispute guard to avoid connectivity loss in VLAN networks. As shown in Figure 47, the spanning tree feature is disabled on Device B and enabled on Device A and device C. Device B transparently transmits BPDUs.

Device C cannot receive superior BPDUs of VLAN 1 from Device A because Port B1 of Device B is configured to deny packets of VLAN 1. Device C determines itself as the root bridge after a certain period of time. Then, Port C1 sends an inferior BPDU of VLAN 100 to Device A.

When Device A receives the inferior BPDU, dispute guard blocks Port A1, which causes traffic interruption. To ensure service continuity, you can disable dispute guard on Device A to prevent the link from being blocked.

**Figure 47 Disabling dispute guard application scenario**

Disabling dispute guard might cause loops. Make sure the network is loop-free when you disable dispute guard.

To disable dispute guard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable dispute guard.</td>
<td>undo stp dispute-protection</td>
</tr>
</tbody>
</table>
### Enabling the device to log events of detecting or receiving TC BPDUs

This feature allows the device to generate logs when it detects or receives TC BPDUs. This feature applies only to PVST mode.

To enable the device to log events of detecting or receiving TC BPDUs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>stp log enable tc</td>
<td>By default, the device does not generate logs when it detects or receives TC BPDUs.</td>
</tr>
</tbody>
</table>

### Disabling the device to reactivate the shutdown edge ports

A device enabled with BPDU guard shuts down edge ports that have received configuration BPDUs and notifies the NMS of the shutdown event. After a port status detection interval, the device reactivates the shutdown ports. This feature allows you to disable the device to reactivate the shutdown ports. The feature applies to edge ports that are shut down after you configure the `stp port shutdown permanent` command. To bring up these ports, use the `undo shutdown` command.

For more information about the port status detection interval, see device management configuration in Fundamentals Configuration Guide.

To disable the device to reactivate the shutdown edge ports:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Disable the device to reactivate the shutdown edge ports.</td>
<td>stp port shutdown permanent</td>
<td>By default, a device reactivates the shutdown edge ports after a port status detection interval.</td>
</tr>
</tbody>
</table>

### Enabling BPDPU transparent transmission on a port

Perform this task on the traffic incoming and outgoing ports of PEs in a VPLS network to exclude the PEs from the spanning tree calculation on CEs. Whether the spanning tree protocols are enabled on a port does not affect the BPDPU transparent transmission feature.

If this feature and the spanning tree protocol are enabled on a port which is inferior to its downstream port, the downstream port can receive BPDUs from that port. To prevent network flapping caused by this problem, disable the spanning tree protocol before you enable BPDPU transparent transmission on the port.
To enable transparent transmission on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>stp transparent enable</td>
<td>By default, the BPDU transparent transmission feature is disabled on a port.</td>
</tr>
</tbody>
</table>

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

This task 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` enables SNMP notifications for spanning tree topology changes.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | In STP, MSTP, or RSTP mode, execute either of the following commands:  
  - `snmp-agent trap enable stp new-root`  
  - `snmp-agent trap enable stp tc` | The default settings are as follows:  
  - 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.   | In PVST mode, execute either of the following commands:  
  - `snmp-agent trap enable stp tc`  
  - `snmp-agent trap enable stp` | |

### Displaying and maintaining the spanning tree

Execute `display` commands in any view and `reset` command in user view.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display history about ports blocked by spanning tree protection features.</td>
<td><code>display stp abnormal-port</code></td>
</tr>
<tr>
<td>Display BPDU statistics on ports.</td>
<td><code>display stp bpdu-statistics [ interface interface-type interface-number [ instance instance-list ] ]</code></td>
</tr>
<tr>
<td>Display information about ports shut down by spanning tree protection features.</td>
<td><code>display stp down-port</code></td>
</tr>
<tr>
<td>Display the port role calculation history for the specified MSTI or all MSTIs.</td>
<td><code>display stp [ instance instance-list ] [ vlan vlan-id-list ] history [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display the incoming and outgoing TC/TCN BPDU statistics by all ports in the specified MSTI or all MSTIs.</td>
<td><code>display stp [ instance instance-list ] [ vlan vlan-id-list ] tc [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display the spanning tree status and statistics.</td>
<td>`display stp [ instance instance-list ] [ vlan vlan-id-list ] [ interface interface-list</td>
</tr>
<tr>
<td>Display the MST region configuration information that has taken effect.</td>
<td><code>display stp region-configuration</code></td>
</tr>
<tr>
<td>Display the root bridge information of all MSTIs.</td>
<td><code>display stp root</code></td>
</tr>
<tr>
<td>Clear the spanning tree statistics.</td>
<td><code>reset stp [ interface interface-list ]</code></td>
</tr>
</tbody>
</table>

**Spanning tree configuration examples**

**MSTP configuration example**

**Network requirements**

As shown in Figure 48, 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 frames of different VLANs are forwarded along different spanning trees.

- VLAN 10 frames are forwarded along MSTI 1.
- VLAN 30 frames are forwarded along MSTI 3.
- VLAN 40 frames are forwarded along MSTI 4.
- VLAN 20 frames 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.
**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
   - # Configure the Device A 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.

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
   # Configure Device C 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, you can 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
MST ID  Port                         Role  STP State     Protection
0       Ten-GigabitEthernet1/0/1     ALTE  DISCARDING    NONE
0       Ten-GigabitEthernet1/0/2     DESI  FORWARDING    NONE
0       Ten-GigabitEthernet1/0/3     ROOT  FORWARDING    NONE
1       Ten-GigabitEthernet1/0/1     DESI  FORWARDING    NONE
1       Ten-GigabitEthernet1/0/3     ROOT  FORWARDING    NONE
3       Ten-GigabitEthernet1/0/2     DESI  FORWARDING    NONE
3       Ten-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       Ten-GigabitEthernet1/0/1     DESI  FORWARDING    NONE
0       Ten-GigabitEthernet1/0/2     DESI  FORWARDING    NONE
0       Ten-GigabitEthernet1/0/3     DESI  FORWARDING    NONE
1       Ten-GigabitEthernet1/0/2     DESI  FORWARDING    NONE
1       Ten-GigabitEthernet1/0/3     ROOT  FORWARDING    NONE
3       Ten-GigabitEthernet1/0/1     DESI  FORWARDING    NONE
3       Ten-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       Ten-GigabitEthernet1/0/1     DESI  FORWARDING    NONE
0       Ten-GigabitEthernet1/0/2     ROOT  FORWARDING    NONE
0       Ten-GigabitEthernet1/0/3     DESI  FORWARDING    NONE
1       Ten-GigabitEthernet1/0/1     ROOT  FORWARDING    NONE
1       Ten-GigabitEthernet1/0/2     ALTE  DISCARDING    NONE
4       Ten-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       Ten-GigabitEthernet1/0/1     ROOT  FORWARDING    NONE
0       Ten-GigabitEthernet1/0/2     ALTE  DISCARDING    NONE
0       Ten-GigabitEthernet1/0/3     ALTE  DISCARDING    NONE
3       Ten-GigabitEthernet1/0/1     ROOT  FORWARDING    NONE
3       Ten-GigabitEthernet1/0/2     ALTE  DISCARDING    NONE
4       Ten-GigabitEthernet1/0/3     ROOT  FORWARDING    NONE
```

Based on the output, you can draw each MSTI mapped to each VLAN, as shown in Figure 49.
PVST configuration example

Network requirements

As shown in Figure 50, Device A and Device B work at the distribution layer, and Device C and Device D work at the access layer.

Configure PVST to meet the following requirements:

- Frames 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.
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
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, you can 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

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>10</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>30</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>30</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
</tbody>
</table>

# Display brief spanning tree information on Device B.

[DeviceB] display stp brief

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>10</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>30</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>30</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
</tbody>
</table>

# Display brief spanning tree information on Device C.

[DeviceC] display stp brief

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>10</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>40</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
</tbody>
</table>

# Display brief spanning tree information on Device D.

[DeviceD] display stp brief

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/2</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>20</td>
<td>Ten-GigabitEthernet1/0/3</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>30</td>
<td>Ten-GigabitEthernet1/0/1</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
</tbody>
</table>
Based on the output, you can draw a topology for each VLAN spanning tree, as shown in Figure 51.

Figure 51 VLAN spanning tree topologies

![Diagram of VLAN spanning tree topologies]

**Configuring DRNI with PVST**

**Network configuration**

As shown in Figure 52, Device A and Device B work at the distribution layer, and Device C and Device D work at the access layer.

Configure DRNI on Device A and Device B. In the DR system, Device A is the primary DR device, and Device B is the secondary DR device.

Configure PVST on the devices to meet the following requirements:

- Frames 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.
- The root bridge of VLAN 10, VLAN 20, and VLAN 30 is the DR system formed by Device A and Device B.

**NOTE:**

As a best practice, do not connect ports on Device A and Device B that have the same port ID with each other, including Layer 2 aggregate interfaces. Otherwise, when Device A and Device B communicate through the link, the spanning tree protocol determines that the device receives its own BPDUs. Loop guard will block the link, though spanning tree features are not affected.

You can view port IDs of interfaces on the device by using the `display stp interface` command.

The above restrictions do not apply to IPPs and their member ports.
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, and VLAN 20 on Device C.
   - Create VLAN 20, and VLAN 30 on Device D.
   - Configure the ports on these devices as trunk ports and assign them to related VLANs.

2. Configure DRNI on Device A and Device B. (Details not shown.)
   For more information about DRNI, see "Configuring DRNI."

3. 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

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

5. Configure Device C:
   # Set the spanning tree mode to PVST.
   <DeviceC> system-view
   [DeviceC] stp mode pvst
   # Enable the spanning tree feature globally and in VLAN 10, and VLAN 20.
   [DeviceC] stp global enable
   [DeviceC] stp vlan 10 20 enable

6. 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, and VLAN 30.
   [DeviceD] stp global enable
   [DeviceD] stp vlan 20 30 enable
Verifying the configuration

When the network is stable, you can use the `display stp brief` command to display brief spanning tree information on each device.

# Display brief spanning tree information of the DR system on the primary DR device, Device A.

```
[DeviceA] display stp brief
VLAN ID   Port             Role  STP State     Protection
10         Bridge-Aggregation1  DESI  FORWARDING    NONE
20         Bridge-Aggregation1  DESI  FORWARDING    NONE
20         Bridge-Aggregation2  DESI  FORWARDING    NONE
30         Bridge-Aggregation2  DESI  FORWARDING    NONE
```

# Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
VLAN ID   Port             Role  STP State     Protection
10         Bridge-Aggregation1  ROOT  FORWARDING    NONE
20         Bridge-Aggregation1  ROOT  FORWARDING    NONE
```

# Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
VLAN ID   Port             Role  STP State     Protection
20         Bridge-Aggregation2  ROOT  FORWARDING    NONE
30         Bridge-Aggregation2  ROOT  FORWARDING    NONE
```
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 transmissions can waste network resources and can 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 different VLAN tag than it was sent out with, an inter-VLAN loop has occurred. To remove the loop, examine the QinQ or VLAN mapping configuration for incorrect settings. For more information about QinQ and VLAN mapping, see "Configuring QinQ" and "Configuring VLAN mapping."

Figure 53 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 performs the following operations:
  - Sends the frame to the CPU.
  - 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 54 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 13 TLVs supported by loop detection

<table>
<thead>
<tr>
<th>TLV</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>End of PDU</td>
<td>End of a PDU.</td>
<td>Optional.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Bridge MAC address of the sending device.</td>
<td>Required.</td>
</tr>
<tr>
<td>Port ID</td>
<td>ID of the PDU sending port.</td>
<td>Optional.</td>
</tr>
<tr>
<td>Port Name</td>
<td>Name of the PDU sending port.</td>
<td>Optional.</td>
</tr>
<tr>
<td>System Name</td>
<td>Device name.</td>
<td>Optional.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis ID of the sending port.</td>
<td>Optional.</td>
</tr>
<tr>
<td>Slot ID</td>
<td>Slot ID of the sending port.</td>
<td>Optional.</td>
</tr>
<tr>
<td>Sub Slot ID</td>
<td>Sub-slot ID of the sending port.</td>
<td>Optional.</td>
</tr>
</tbody>
</table>

**Loop detection interval**

Loop detection is a continuous process as the network changes. Loop detection frames are sent at the loop detection interval to determine whether loops occur on ports and whether loops are removed.

**Loop protection actions**

When the device detects a loop on a port, it generates a log but performs no action on the port by default. You can configure the device to take one of the following actions:

- **Block**—Disables the port from learning MAC addresses and blocks 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 operations:

- 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 set 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, use the shutdown action, or manually remove the loop.

## Loop detection configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling loop detection</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Setting the loop protection action</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Setting the loop detection interval</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling loop detection

The loop protection action on a port can be triggered even if loop detection is disabled on the port when the following requirements are met:

- Loop detection is enabled globally or on any other port on the device.
- The port receives a loop detection frame of any VLAN.

As a best practice, do not enable loop detection on TRILL ports, because TRILL networks prevent loops from being generated. For information more about TRILL, see *TRILL Configuration Guide*.

When EVB is enabled on a Layer 2 Ethernet interface or Layer 2 aggregate interface, the loop detection feature does not take effect on the interface.

### Enabling loop detection globally

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Globally enable loop detection.</td>
<td>`loopback-detection global enable vlan { vlan-id--list</td>
</tr>
</tbody>
</table>

### Enabling loop detection on a port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
</tbody>
</table>
### Setting the loop protection action

You can set the loop protection action globally or on a per-port basis. The global setting applies to all ports. The per-port setting applies to the individual ports. The per-port setting takes precedence over the global setting.

#### Setting the global loop protection action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the global loop protection action.</td>
<td>loopback-detection global action shutdown</td>
<td>By default, the device generates a log but performs no action on the port on which a loop is detected.</td>
</tr>
</tbody>
</table>

#### Setting the loop protection action on a Layer 2 Ethernet interface or S-channel interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view or S-channel interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the loop protection action on the interface.</td>
<td>loopback-detection action { block</td>
<td>no-learning</td>
</tr>
</tbody>
</table>

#### Setting the loop protection action on a Layer 2 aggregate interface, S-channel aggregate interface, or S-channel bundle interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 aggregate interface view, S-channel aggregate interface view, or S-channel bundle interface</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Setting the loop detection interval

With loop detection enabled, the device sends loop detection frames at the loopback detection 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>loopback-detection interval-time <em>interval</em></td>
<td>The default setting is 30 seconds.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining loop detection

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the loop detection configuration and status.</td>
<td>display loopback-detection</td>
</tr>
</tbody>
</table>

### Loop detection configuration example

**Network requirements**

As shown in Figure 55, configure loop detection on Device A to meet the following requirements:

- Device A generates a log as a notification.
- Device A automatically shuts down the port on which a loop is detected.
Figure 55 Network diagram

Configuration procedure

1. Configure Device A:
   # Create VLAN 100, and globally enable loop detection for the VLAN.
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] quit
   [DeviceA] loopback-detection global enable vlan 100
   # Configure Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 as trunk ports, and
   # assign them to VLAN 100.
   [DeviceA] interface Ten-GigabitEthernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-type trunk
   [DeviceA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-type trunk
   [DeviceA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   # Set the global loop protection action to 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 as trunk ports, and
   # assign them to VLAN 100.
   [DeviceB] interface ten-gigabitethernet 1/0/1
Configure Device B:
[DeviceB-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-Ten-GigabitEthernet1/0/1] quit
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-Ten-GigabitEthernet1/0/2] quit

3. Configure Device C:

# Create VLAN 100.
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC-vlan100] quit

# Configure Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 as trunk ports, and assign them to VLAN 100.
[DeviceC] interface ten-gigabitethernet 1/0/1
[DeviceC-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-Ten-GigabitEthernet1/0/1] quit
[DeviceC] interface ten-gigabitethernet 1/0/2
[DeviceC-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceC-Ten-GigabitEthernet1/0/2] quit

Verifying the configuration

# View the system logs on devices, for example, Device A.
[DeviceA]

The output shows the following information:
- Device A detected loops on Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 within a loop detection interval.
- Loops on Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 were removed.

# (Available in Release 2609.) 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 according to the shutdown action.
# (Available in R2612 and later.) Use the `display loopback-detection` command to display the loop detection configuration and status on devices, for example, Device A.

```
[DeviceA] display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 35 second(s).
Loopback is detected on following interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Action mode</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ten-GigabitEthernet1/0/1</td>
<td>Shutdown</td>
<td>100</td>
</tr>
<tr>
<td>Ten-GigabitEthernet1/0/2</td>
<td>Shutdown</td>
<td>100</td>
</tr>
</tbody>
</table>
```

The output shows that the device has removed the loops from Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 in VLAN 100 by shutting the interfaces down.

# Display the status of Ten-GigabitEthernet 1/0/1 on devices, for example, Device A.
```
[DeviceA] display interface ten-gigabitethernet 1/0/1
Ten-GigabitEthernet1/0/1 current state: DOWN (Loop detection down)
... 
```

The output shows that Ten-GigabitEthernet 1/0/1 is already shut down by the loop detection module.

# Display the status of Ten-GigabitEthernet 1/0/2 on devices, for example, Device A.
```
[DeviceA] display interface ten-gigabitethernet 1/0/2
Ten-GigabitEthernet1/0/2 current state: DOWN (Loop detection down)
... 
```

The output shows that Ten-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 56.

Figure 56 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 the Type field.

Figure 57 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 hexadecimal TPID value 8100 identifies a VLAN-tagged frame. A device vendor can set the
TPID to a different value. For compatibility with a neighbor device, set the TPID value on the
device to be the same as the neighbor device. For more information about setting the TPID
value, see "Configuring QinQ."

- **Priority**—3-bit long, identifies the 802.1p priority of the frame. For more information, see *ACL
and QoS Configuration Guide*.

- **CFI**—1-bit long canonical format indicator that indicates whether the MAC addresses are
encapsulated in the standard format when packets are transmitted across different media.
Available values include:
  
  - **0 (default)**—The MAC addresses are encapsulated in the standard format.
  - **1**—The MAC addresses are encapsulated in a non-standard format.

  This field is always set to 0 for Ethernet.

- **VLAN ID**—12-bit long, identifies the VLAN to which the frame belongs. The VLAN ID range is 0
to 4095. VLAN IDs 0 and 4095 are reserved, and VLAN IDs 1 to 4094 are user configurable.

The way a network device handles an incoming frame depends on whether the frame has a VLAN
tag and the value of the VLAN tag (if any). For more information, see "Introduction."

Ethernet supports encapsulation formats Ethernet II, 802.3/802.2 LLC, 802.3/802.2 SNAP, and
802.3 raw. The Ethernet II encapsulation format is used here. For information about the VLAN tag
fields in other frame encapsulation formats, see related protocols and standards.

For a frame that has multiple VLAN tags, the device handles it according to its outermost VLAN tag
and transmits its inner VLAN tags as the payload.

### Protocols and standards

*IEEE 802.1Q, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area
Networks*

### Configuring a VLAN

When you configure a VLAN, follow these restrictions and guidelines:

- As the system default VLAN, VLAN 1 cannot be created or deleted.
- Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove
  the configuration from the VLAN.

To configure a VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Create a VLAN and enter its view, or create a list of VLANs.</td>
<td>`vlan { vlan-id-list</td>
</tr>
<tr>
<td>3.</td>
<td>Enter VLAN view.</td>
<td><code>vlan vlan-id</code></td>
</tr>
</tbody>
</table>
| 4. | Set a name for the VLAN. | `name text` | By default, the name of a VLAN is **VLAN vlan-id**. The `vlan-id` 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**. |
<p>| 5. | Configure the description for the | <code>description text</code> | By default, the description of a VLAN is <strong>VLAN vlan-id</strong>. The <code>vlan-id</code> argument |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN.</td>
<td>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 <strong>VLAN 0100</strong>.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Enable packet dropping in the VLAN.</td>
<td>By default, packet dropping is disabled in a VLAN. This feature enables the device to drop packets (including protocol packets) forwarded by the software in a VLAN. To drop all packets that are received and transmitted in the VLAN, you must configure a QoS policy. For more information about configuring QoS policies, see <em>ACL and QoS Configuration Guide</em>.</td>
</tr>
</tbody>
</table>

### Configuring VLAN interfaces

Hosts of different VLANs use VLAN interfaces to communicate at Layer 3. VLAN interfaces are virtual interfaces that do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface and assign an IP address to it. The VLAN interface acts as the gateway of the VLAN to forward packets destined for another IP subnet at Layer 3.

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 VLAN interfaces for sub-VLANs. For more information about sub-VLANs, see "Configuring super VLANs."
- You cannot create VLAN interfaces for secondary VLANs that have the following characteristics:
  - Associated with the same primary VLAN.
  - Enabled with Layer 3 communication in VLAN interface view of the primary VLAN interface.
  For more information about secondary VLANs, see "Configuring the private VLAN."
- To associate a VPN instance with a VLAN interface, make sure one or more of the following conditions are met:
  - A Layer 3 Ethernet subinterface and a Layer 3 aggregate subinterface that have the same number as the VLAN interface are associated with the VPN instance.
  - Packet statistics is enabled on the Layer 3 Ethernet subinterface.
  - Packet statistics is enabled on the Layer 3 aggregate subinterface.
  For more information about Layer 3 Ethernet subinterfaces, see Ethernet interface in *Layer 2—LAN Switching Configuration Guide*. For more information about Layer 3 aggregate subinterfaces, see Ethernet link aggregation in *Layer 2—LAN Switching Configuration Guide*. For more information about associating a VPN instance with an interface, see MPLS L3VPN and MCE in *MPLS Configuration Guide*.
- Configuring a MAC address for a VLAN interface is exclusive with BFD MAD. Make sure BFD MAD is not configured on a VLAN interface before you configure a MAC address for the VLAN interface by using the **mac-address** command. For more information about BFD MAD, see *Virtual Technologies Configuration Guide*.

To configure basic settings of a VLAN interface:
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 set the link type of a port to access, trunk, or hybrid. The port link type determines whether the port can be assigned to multiple VLANs. The link types use the following VLAN tag handling methods:

- **Access**—An access port can forward packets only from one VLAN and send these packets untagged. An access port is typically used in the following conditions:
  - Connecting to a terminal device that does not support VLAN packets.
  - In scenarios that do not distinguish VLANs.

- **Trunk**—A trunk port can forward packets from multiple VLANs. Except packets from the port VLAN ID (PVID), packets sent out of a trunk port are VLAN-tagged. Ports connecting network devices are typically configured as trunk ports.

- **Hybrid**—A hybrid port can forward packets from multiple VLANs. The tagging status of the packets forwarded by a hybrid port depends on the port configuration. In one-to-two VLAN mapping, hybrid ports are used to remove SVLAN tags for downlink traffic. For more information about one-to-two VLAN mapping, see "Configuring VLAN mapping."
PVID

The PVID identifies the default VLAN of a port. Untagged packets received on a port are considered as the packets from the port PVID.

When you set the PVID for a port, follow these restrictions and guidelines:

- An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port.
- A trunk or hybrid port supports multiple VLANs and the PVID configuration.
- When you use the `undo vlan` command to delete the PVID of a port, either of the following events occurs depending on the port link type:
  - For an access port, the PVID of the port changes to VLAN 1.
  - For a hybrid or trunk port, the PVID setting of the port does not change.
  You can use a nonexistent VLAN as the PVID for a hybrid or trunk port, but not for an access port.
- As a best practice, set the same PVID for a local port and its peer.
- To prevent a port from dropping untagged packets or PVID-tagged packets, assign the port to its PVID.

How ports of different link types handle frames

<table>
<thead>
<tr>
<th>Actions</th>
<th>Access</th>
<th>Trunk</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the inbound direction for an untagged frame</td>
<td>Tags the frame with the PVID tag.</td>
<td>• If the PVID is permitted on the port, tags the frame with the PVID tag.</td>
<td>Sends the frame if its VLAN is permitted on the port. The tagging status of the frame depends on the <code>port hybrid vlan</code> command configuration.</td>
</tr>
<tr>
<td>In the inbound direction for a tagged frame</td>
<td>• Receives the frame if its VLAN ID is the same as the PVID. • Drops the frame if its VLAN ID is different from the PVID.</td>
<td>• Receives the frame if its VLAN is permitted on the port. • Drops the frame if its VLAN is not permitted on the port.</td>
<td></td>
</tr>
<tr>
<td>In the outbound direction</td>
<td>Removes the VLAN tag and sends the frame.</td>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

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.

Assign one or multiple access ports to a VLAN in VLAN view

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Assign one or multiple access ports to the VLAN.</td>
<td>port interface-list</td>
</tr>
</tbody>
</table>

Assign an access port to a VLAN in interface view

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view. | • Enter Layer 2 Ethernet interface view: `interface interface-type interface-number`  
• Enter Layer 2 aggregate interface view: `interface bridge-aggregation interface-number`  
• Enter S-channel interface view: `interface s-channel interface-number.channel-id`  
• Enter S-channel aggregate interface view: `interface schannel-aggregation interface-number.channel-id`  
• Enter S-channel bundle interface view: `interface schannel-bundle interface-number` | N/A |
| 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 vlan-id | By default, all access ports belong to VLAN 1. |

Assigning a trunk port to a VLAN

A trunk port supports multiple VLANs. You can assign it to a VLAN in interface view.

When you assign a trunk port to a VLAN, follow these restrictions and guidelines:

- To change the link type of a port from trunk to hybrid, 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:
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, 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:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td><code>interface-number</code>&lt;br&gt;<code>port link-type hybrid</code></td>
<td>By default, all ports are access ports.</td>
</tr>
<tr>
<td>4.</td>
<td>`port hybrid vlan vlan-id-list { tagged</td>
<td>untagged }`</td>
</tr>
<tr>
<td>5.</td>
<td><code>(Optional.) </code>port hybrid pvid vlan vlan-id`</td>
<td>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.</td>
</tr>
</tbody>
</table>

## 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 also called user-based VLAN because VLAN configuration remains the same regardless of a user's physical location.

### Static MAC-based VLAN assignment

Use static MAC-based VLAN assignment in networks that have a small number of VLAN users. To configure static MAC-based VLAN assignment on a port, perform the following tasks:

1. Create MAC-to-VLAN entries.
2. Enable the MAC-based VLAN feature on the port.
3. Assign the port to the MAC-based VLAN.

A port configured with static MAC-based VLAN assignment processes a received frame as follows before sending the frame out:

- For an untagged frame, the port determines its VLAN ID in the following workflow:
  a. The port first performs a fuzzy match as follows:
     - Searches for the MAC-to-VLAN entries whose masks are not all Fs.
     - Performs a logical AND operation on the source MAC address and each of these masks.
     - If an AND operation result matches the MAC address in a MAC-to-VLAN entry, the port tags the frame with the VLAN ID specific to this entry.
  b. If the fuzzy match fails, the port performs an exact match. It searches for MAC-to-VLAN entries whose masks are all Fs. If the source MAC address of the frame exactly matches the MAC address of a MAC-to-VLAN entry, the port tags the frame with the VLAN ID specific to this entry.
  c. If no matching VLAN ID is found, the port determines the VLAN for the packet by using the following VLAN match order:
     - IP subnet-based VLAN.
     - Protocol-based VLAN.
     - Port-based VLAN.
When a match is found, the port tags the packet with the matching VLAN ID.

- For a tagged frame, the port determines whether the VLAN ID of the frame is permitted on the port.
  - If the VLAN ID of the frame is permitted on the port, the port forwards the frame.
  - If the VLAN ID of the frame is not permitted on the port, the port drops the frame.

**Dynamic MAC-based VLAN assignment**

When you cannot determine the target MAC-based VLANs of a port, use dynamic MAC-based VLAN assignment on the port. To use dynamic MAC-based VLAN assignment, perform the following tasks:

1. Create MAC-to-VLAN entries.
2. Enable the MAC-based VLAN feature on the port.
3. Enable dynamic MAC-based VLAN assignment on the port.

Dynamic MAC-based VLAN assignment uses the following workflow, as shown in Figure 58:

4. When a port receives a frame, it first determines whether the frame is tagged.
   - If the frame is tagged, the port gets 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 (fuzzy and exact MAC address match).
     - IP subnet-based VLAN.
     - Protocol-based VLAN.
     - Port-based VLAN.
   After tagging the frame with the selected VLAN, the port gets the source MAC address of the frame.
5. The port uses the source address and VLAN of the frame to match the MAC-to VLAN entries.
   - If the source MAC address of the frame exactly matches the MAC address in a MAC-to-VLAN entry, the port checks whether the VLAN ID of the frame matches the VLAN in the entry.
     - If the two VLAN IDs match, the port joins the VLAN and forwards the frame.
     - If the two VLAN IDs do not match, the port drops the frame.
   - If the source MAC address of the frame does not exactly match any MAC addresses in MAC-to-VLAN entries, 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 determines whether the VLAN ID is the primary VLAN ID and the port PVID is a secondary VLAN ID.
       - If yes, the port forwards the frame. Otherwise, the port drops the frame.
When you configure dynamic MAC-based VLAN assignment, follow these guidelines:

- When a port joins a VLAN specified in the MAC-to-VLAN entry, one of the following events occurs depending on the port configuration:
  - If the port has not been configured to allow packets from the VLAN to pass through, the port joins the VLAN as an untagged member.
  - If the port has been configured to allow packets from the VLAN to pass through, the port configuration remains the same.

- If you configure both static and dynamic MAC-based VLAN assignments on a port, dynamic MAC-based VLAN assignment takes effect.
- The 802.1p priority of the VLAN in a MAC-to-VLAN entry determines the transmission priority of the matching packets.

**Server-assigned MAC-based VLAN**

Use this feature with access authentication, such as MAC-based 802.1X authentication, to implement secure and flexible terminal access.

To implement server-assigned MAC-based VLAN, perform the following tasks:

1. Configure the server-assigned MAC-based VLAN feature on the access device.
2. Configure username-to-VLAN entries on the access authentication server.

When a user passes authentication of the access authentication server, the server assigns the authorization VLAN information for the user to the device. The device then performs the following operations:

3. Generates a MAC-to-VLAN entry by using the source MAC address of the user packet and the authorization VLAN information. The authorization VLAN is a MAC-based VLAN. The generated MAC-to-VLAN entry cannot conflict with the existing static MAC-to-VLAN entries. If a confliction exists, the dynamic MAC-to-VLAN entry cannot be generated.
4. 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.

General configuration restrictions and guidelines

When you configure MAC-based VLANs, follow these restrictions and guidelines:
- Do not configure a VLAN as both a super VLAN and a MAC-based VLAN.
- The MAC-based VLAN feature is mainly configured on downlink ports of user access devices. Do not use this feature with link aggregation.

Configuring static MAC-based VLAN assignment

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 Ethernet interface view:</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel interface view:</td>
<td>interface s-channel interface-number.channel-id</td>
</tr>
<tr>
<td></td>
<td>• Enter S-channel aggregate interface view:</td>
<td>interface schannel-aggregation interface-number.channel-id</td>
</tr>
<tr>
<td>4.</td>
<td>Set the port link type to hybrid.</td>
<td>port link-type hybrid</td>
</tr>
<tr>
<td>5.</td>
<td>Assign the hybrid port to the MAC-based VLANs.</td>
<td>port hybrid vlan vlan-id-list { tagged</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the MAC-based VLAN feature.</td>
<td>mac-vlan enable</td>
</tr>
<tr>
<td>7.</td>
<td>(Optional.) Configure the system to assign VLANs based on the MAC address preferentially.</td>
<td>vlan precedence mac-vlan</td>
</tr>
</tbody>
</table>

Configuring dynamic MAC-based VLAN assignment

Configuration restrictions and guidelines

When you configure dynamic MAC-based VLAN assignment, follow these restrictions and guidelines:
• As a best practice to ensure correct operation of 802.1X and MAC authentication, do not use dynamic MAC-based VLAN assignment with 802.1X or MAC authentication.

• As a best practice, do not both configure dynamic MAC-based VLAN assignment and disable MAC address learning on a port. If the two features are configured together on a port, the port forwards only packets exactly matching the MAC-to-VLAN entries and drops inexact matching packets.

• As a best practice, do not configure both dynamic MAC-based VLAN assignment and the MAC learning limit on a port.

  If the two features are configured together on a port and the port learns the configured maximum number of MAC address entries, the port processes packets as follows:
  o Forwards only packets matching the MAC address entries learnt by the port.
  o Drops unmatching packets.

• For successful dynamic MAC-based VLAN assignment, use static VLANs when you create MAC-to-VLAN entries.

• As a best practice, do not use dynamic MAC-based VLAN assignment with MSTP. In MSTP mode, if a port is blocked in the MSTI of its target VLAN, the port drops the received packets instead of delivering them to the CPU. As a result, the port will not be dynamically assigned to the target VLAN.

• As a best practice, do not use dynamic MAC-based VLAN assignment with PVST. In PVST mode, if the target VLAN of a port is not permitted on the port, the port is placed in blocked state. The port drops the received packets instead of delivering them to the CPU. As a result, the port will not be dynamically assigned to the target VLAN.

• As a best practice, do not configure both dynamic MAC-based VLAN assignment and automatic voice VLAN assignment mode on a port. They can have a negative impact on each other.

**Configuration procedure**

To configure dynamic MAC-based VLAN assignment:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a MAC-to-VLAN entry.</td>
<td>mac-vlan mac-address vlan vlan-id [ dot1q priority ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>• Enter Layer 2 Ethernet interface view:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter S-channel interface view:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface s-channel interface-number.channel-id</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter S-channel aggregate interface view:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface s-channel-aggregation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-number.channel-id</td>
</tr>
<tr>
<td>4.</td>
<td>Set the port link type to hybrid.</td>
<td>port link-type hybrid</td>
</tr>
<tr>
<td>5.</td>
<td>Enable the MAC-based VLAN feature.</td>
<td>mac-vlan enable</td>
</tr>
<tr>
<td>6.</td>
<td>Enable dynamic MAC-based VLAN assignment.</td>
<td>mac-vlan trigger enable</td>
</tr>
</tbody>
</table>
### Configuring server-assigned MAC-based VLAN

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view. | • Enter Layer 2 Ethernet interface view:  
  *interface*  
  *interface-type*  
  *interface-number*  
  • Enter S-channel interface view:  
  *interface s-channel*  
  *interface-number.channel-id*  
  • Enter S-channel aggregate interface view:  
  *interface s-channel-aggregation*  
  *interface-number.channel-id* | N/A |
| 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 MAC-based VLANs. | port hybrid vlan  
  *vlan-id-list*  
  { tagged | untagged } | By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access. |
| 5.   | Enable the MAC-based VLAN feature. | mac-vlan enable | By default, MAC-based VLAN is disabled. |
| 6.   | Configure 802.1X or MAC authentication. | For more information, see Security Command Reference. | N/A |

### Configuring IP subnet-based VLANs

In this method, untagged 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 untagged packets from an IP subnet or IP address must be transmitted in a VLAN.
This feature is available only on hybrid ports, and it processes only untagged packets.

An IP subnet-based VLAN has one or multiple subnets to match inbound packets. Each subnet has a unique index in the IP subnet-based VLAN. All subnets in an IP subnet-based VLAN have the same VLAN ID.

To configure an IP subnet-based VLAN:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter VLAN view.</td>
<td>vlan vlan-id</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Associate the VLAN with an IP subnet or IP address.</td>
<td>ip-subnet-vlan [ ip-subnet-index ] ip-ip-address [ mask ]</td>
<td>By default, a VLAN is not associated with an IP subnet or IP address. A multicast subnet or a multicast address cannot be associated with a VLAN.</td>
</tr>
<tr>
<td>4. Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>5. Enter interface view.</td>
<td>• Enter Layer 2 Ethernet interface view. interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view. interface bridge-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td>6. Set the port link type to hybrid.</td>
<td>port link-type hybrid</td>
<td>By default, all ports are access ports.</td>
</tr>
<tr>
<td>7. Assign the hybrid port to the specified IP subnet-based VLANs.</td>
<td>port hybrid vlan vlan-id-list ( tagged</td>
<td>untagged )</td>
</tr>
<tr>
<td>8. Associate the hybrid port with the specified IP subnet-based VLAN.</td>
<td>port hybrid ip-subnet-vlan vlan vlan-id</td>
<td>By default, a hybrid port is not associated with a subnet-based VLAN.</td>
</tr>
</tbody>
</table>

Configuring protocol-based VLANs

The protocol-based VLAN feature assigns inbound packets to different VLANs based on their protocol types and encapsulation formats. The protocols available for VLAN assignment include IP, IPX, and AT. The encapsulation formats include Ethernet II, 802.3 raw, 802.2 LLC, and 802.2 SNAP.

This feature is available only on hybrid ports, and it processes only untagged packets. It associates the available network service types with VLANs and facilitates network management and maintenance.

A protocol-based VLAN has one or multiple protocol templates. A protocol template defines a protocol type and an encapsulation format as the match criteria to match inbound packets. Each protocol template has a unique index in the protocol-based VLAN. All protocol templates in a protocol-based VLAN have the same VLAN ID.

For a port to assign inbound packets to protocol-based VLANs, perform the following tasks:

- Assign the port to the protocol-based VLANs.
- Associate the port with the protocol templates of the protocol-based VLANs.

When an untagged packet arrives at the port, the port processes the packet as follows:
- If the protocol type and encapsulation format in the packet match a protocol template, the port tags the packet with the VLAN tag specific to the protocol template.
- If no protocol templates are matched, the port tags the packet with its PVID.

The voice VLAN in automatic mode processes only tagged voice traffic. Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN.

To configure a protocol-based VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Associate the VLAN with a protocol template.</td>
<td>protocol-vlan [ protocol-index ] { at</td>
</tr>
<tr>
<td>4.</td>
<td>Exit VLAN view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Set the port link type to hybrid.</td>
<td>port link-type hybrid</td>
</tr>
<tr>
<td>7.</td>
<td>Assign the hybrid port to the specified protocol-based VLANs.</td>
<td>port hybrid vlan vlan-id-list { tagged</td>
</tr>
<tr>
<td>8.</td>
<td>Associate the hybrid port with the specified protocol-based VLAN.</td>
<td>port hybrid protocol-vlan vlan { protocol-index [ to protocol-end ]</td>
</tr>
</tbody>
</table>

### 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 or MAC authentication user passes authentication, the authentication server assigns a VLAN group name to the device. If the received VLAN group name matches a locally configured VLAN group name on the device, the device assigns a VLAN in the group to the user. For more information about 802.1X and MAC authentication, see Security Configuration Guide.

To configure a VLAN group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VLAN group and enter its view.</td>
<td>vlan-group group-name</td>
</tr>
<tr>
<td>3.</td>
<td>Add VLANs to the VLAN group.</td>
<td>vlan-list vlan-id-list</td>
</tr>
</tbody>
</table>
Displaying and maintaining VLANs

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display VLAN interface information.</td>
<td>`display interface vlan-interface [interface-number] [brief [description</td>
</tr>
<tr>
<td>Display information about IP subnet-based VLANs that are associated with the specified ports.</td>
<td>`display ip-subnet-vlan interface {interface-type interface-number1 [to interface-type interface-number2]</td>
</tr>
<tr>
<td>Display information about IP subnet-based VLANs.</td>
<td>`display ip-subnet-vlan vlan {vlan-id1 [to vlan-id2]</td>
</tr>
<tr>
<td>Display information about protocol-based VLANs that are associated with the specified ports.</td>
<td>`display protocol-vlan interface {interface-type interface-number1 [to interface-type interface-number2]</td>
</tr>
<tr>
<td>Display information about protocol-based VLANs.</td>
<td>`display protocol-vlan vlan {vlan-id1 [to vlan-id2]</td>
</tr>
<tr>
<td>Display VLAN information.</td>
<td>`display vlan [vlan-id1 [to vlan-id2]</td>
</tr>
<tr>
<td>Display brief VLAN information.</td>
<td><code>display vlan brief</code></td>
</tr>
<tr>
<td>Display VLAN group information.</td>
<td><code>display vlan-group [group-name]</code></td>
</tr>
<tr>
<td>Display hybrid ports or trunk ports on the device.</td>
<td>`display port {hybrid</td>
</tr>
<tr>
<td>Clear statistics on a port.</td>
<td><code>reset counters interface vlan-interface [interface-number]</code></td>
</tr>
</tbody>
</table>

VLAN configuration examples

Port-based VLAN configuration example

**Network requirements**

As shown in **Figure 59**:

- 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.
Configuration procedure

1. Configure Device A:
   # Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 to VLAN 100.
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] port ten-gigabitethernet 1/0/1
   [DeviceA-vlan100] quit

   # Create VLAN 200, and assign Ten-GigabitEthernet 1/0/2 to VLAN 200.
   [DeviceA] vlan 200
   [DeviceA-vlan200] port ten-gigabitethernet 1/0/2
   [DeviceA-vlan200] quit

   # Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and assign the port to VLANs 100 and 200.
   [DeviceA] interface ten-gigabitethernet 1/0/3
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-type trunk
   [DeviceA-Ten-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:
   a. Configure Host A and Host C to be on the same IP subnet. For example, 192.168.100.0/24.
   b. 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 and Host D. (Details not shown.)

# Verify that Host B and Host D can ping each other, but they both fail to ping Host A and Host C. (Details not shown.)

# Verify that VLANs 100 and 200 are correctly configured on Device A.

[DeviceA-Ten-GigabitEthernet1/0/3] display vlan 100
VLAN ID: 100
VLAN type: Static
Route interface: Not configured
Description: VLAN 0100
Name: VLAN 0100
Tagged ports:
   Ten-GigabitEthernet1/0/3
Untagged ports:
   Ten-GigabitEthernet1/0/1
MAC-based VLAN configuration example

Network requirements

As shown in Figure 60:

- Ten-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.
- One department uses VLAN 100 and owns Laptop 1. The other department uses VLAN 200 and owns Laptop 2.

Configure MAC-based VLANs, so that Laptop 1 and Laptop 2 can access Server 1 and Server 2, respectively, no matter which meeting room they are used in.

Figure 60 Network diagram

Configuration procedure

1. Configure Device A:
   
   # Create VLANs 100 and 200.
   
   <DeviceA> system-view
   
   [DeviceA] vlan 100
   
   [DeviceA-Ten-GigabitEthernet1/0/3] display vlan 200
   
   VLAN ID: 200
   
   VLAN type: Static
   
   Route interface: Not configured
   
   Description: VLAN 0200
   
   Name: VLAN 0200

   Tagged ports:
   
   Ten-GigabitEthernet1/0/3

   Untagged ports:
   
   Ten-GigabitEthernet1/0/2
# 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 Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged

# Enable the MAC-based VLAN feature on Ten-GigabitEthernet 1/0/1.
[DeviceA-Ten-GigabitEthernet1/0/1] mac-vlan enable
[DeviceA-Ten-GigabitEthernet1/0/1] quit

# Configure the uplink port (Ten-GigabitEthernet 1/0/2) as a trunk port, and assign it to VLANs 100 and 200.
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceA-Ten-GigabitEthernet1/0/2] quit

2. Configure Device B:

# Create VLAN 100, and assign Ten-GigabitEthernet 1/0/3 to VLAN 100.
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port ten-gigabitethernet 1/0/3
[DeviceB-vlan100] quit

# Create VLAN 200 and assign Ten-GigabitEthernet 1/0/4 to VLAN 200.
[DeviceB] vlan 200
[DeviceB-vlan200] port ten-gigabitethernet 1/0/4
[DeviceB-vlan200] quit

# Configure Ten-GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLANs 100 and 200.
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[DeviceB-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLANs 100 and 200.
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceB-Ten-GigabitEthernet1/0/2] quit

3. Configure Device C in the same way as the Device A is configured. (Details not shown.)

Verifying the configuration

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

# Verify the MAC-to-VLAN entries on Device A and Device C, for example, on Device A.
IP subnet-based VLAN configuration example

Network requirements
As shown in Figure 61, 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 61 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

   Total MAC VLAN address count: 2
# Configure Ten-GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLAN 100 as a tagged VLAN member.
[DeviceC] interface ten-gigabitethernet 1/0/2
[DeviceC-Ten-GigabitEthernet1/0/2] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/2] port hybrid vlan 100 tagged
[DeviceC-Ten-GigabitEthernet1/0/2] quit

# Configure Ten-GigabitEthernet 1/0/3 as a hybrid port, and assign it to VLAN 200 as a tagged VLAN member.
[DeviceC] interface ten-gigabitethernet 1/0/3
[DeviceC-Ten-GigabitEthernet1/0/3] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/3] port hybrid vlan 200 tagged
[DeviceC-Ten-GigabitEthernet1/0/3] quit

# Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.
[DeviceC] interface ten-gigabitethernet 1/0/1
[DeviceC-Ten-GigabitEthernet1/0/1] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged

# Associate Ten-GigabitEthernet 1/0/1 with the IP subnet-based VLANs 100 and 200.
[DeviceC-Ten-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[DeviceC-Ten-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
[DeviceC-Ten-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

# Verify the IP subnet-based VLAN configuration on Device C.
[DeviceC] display ip-subnet-vlan vlan all
VLAN ID: 100
<table>
<thead>
<tr>
<th>Subnet index</th>
<th>IP address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>192.168.5.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

VLAN ID: 200
<table>
<thead>
<tr>
<th>Subnet index</th>
<th>IP address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>192.168.50.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

# Verify the IP subnet-based VLAN configuration on Ten-GigabitEthernet 1/0/1 of Device C.
[DeviceC] display ip-subnet-vlan interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Subnet index</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0</td>
<td>192.168.5.0</td>
<td>255.255.255.0</td>
<td>Active</td>
</tr>
<tr>
<td>200</td>
<td>0</td>
<td>192.168.50.0</td>
<td>255.255.255.0</td>
<td>Active</td>
</tr>
</tbody>
</table>

Protocol-based VLAN configuration example

Network requirements

As shown in Figure 62:
- 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 62 Network diagram**

![Network diagram](image)

**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 Ten-GigabitEthernet 1/0/3 to VLAN 100.
   ```
   [Device-vlan100] port ten-gigabitethernet 1/0/3
   ```

   # 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 Ten-GigabitEthernet 1/0/4 to VLAN 200.
   ```
   [Device-vlan200] port ten-gigabitethernet 1/0/4
   ```

   # 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
   ```

   # Configure VLAN 100 as a protocol-based VLAN. Create an IPv4 protocol template with the index 1, and create an ARP protocol template with the index 2. (In Ethernet II encapsulation, the protocol type ID for ARP is 0806 in hexadecimal notation.)
   ```
   [Device-vlan100] protocol-vlan 1 ipv4
   ```
# Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port link-type hybrid
[Device-Ten-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged

# Associate Ten-GigabitEthernet 1/0/1 with the IPv4 and ARP protocol templates of VLAN 100 and the IPv6 protocol template of VLAN 200.
[Device-Ten-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 1 to 2
[Device-Ten-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 1
[Device-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.
[Device] interface ten-gigabitethernet 1/0/2
[Device-Ten-GigabitEthernet1/0/2] port link-type hybrid
[Device-Ten-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged

# Associate Ten-GigabitEthernet 1/0/2 with the IPv4 and ARP protocol templates of VLAN 100 and the IPv6 protocol template of VLAN 200.
[Device-Ten-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1 to 2
[Device-Ten-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1
[Device-Ten-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: Ten-GigabitEthernet1/0/1

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Protocol index</th>
<th>Protocol type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1</td>
<td>IPv4</td>
<td>Active</td>
</tr>
<tr>
<td>100</td>
<td>2</td>
<td>Ethernet II Etype 0x0806</td>
<td>Active</td>
</tr>
<tr>
<td>200</td>
<td>1</td>
<td>IPv6</td>
<td>Active</td>
</tr>
</tbody>
</table>

Interface: Ten-GigabitEthernet 1/0/2

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Protocol index</th>
<th>Protocol type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1</td>
<td>IPv4</td>
<td>Active</td>
</tr>
<tr>
<td>100</td>
<td>2</td>
<td>Ethernet II Etype 0x0806</td>
<td>Active</td>
</tr>
<tr>
<td>200</td>
<td>1</td>
<td>IPv6</td>
<td>Active</td>
</tr>
</tbody>
</table>
Configuring super VLANs

Hosts in a VLAN typically use IP addresses in the same subnet. For Layer 3 interoperability with other VLANs, you can create a VLAN interface for the VLAN and assign an IP address to it. This requires a large number of IP addresses.

The super VLAN feature was introduced to save IP addresses. A super VLAN is associated with multiple sub-VLANs. These sub-VLANs use the VLAN interface of the super VLAN (also known as a super VLAN interface) as the gateway for Layer 3 communication.

You can create a VLAN interface for a super VLAN and assign an IP address to it. However, you cannot create a VLAN interface for a sub-VLAN. You can assign a physical port to a sub-VLAN, but you cannot assign a physical port to a super VLAN. Sub-VLANs are isolated at Layer 2.

To enable Layer 3 communication between sub-VLANs, perform the following tasks:
1. Create a super VLAN and the VLAN interface for the super VLAN.
2. Enable local proxy ARP or ND on the super VLAN interface as follows:
   - In an IPv4 network, enable local proxy ARP on the super VLAN interface. The super VLAN can then process ARP requests and replies sent from the sub-VLANs.
   - In an IPv6 network, enable local proxy ND on the super VLAN interface. The super VLAN can then process the NS and NA messages sent from the sub-VLANs.

Super VLAN configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Creating a sub-VLAN</td>
<td></td>
</tr>
<tr>
<td>(Required.) Configuring a super VLAN</td>
<td></td>
</tr>
<tr>
<td>(Required.) Configuring a super VLAN interface</td>
<td></td>
</tr>
</tbody>
</table>

Creating a sub-VLAN

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a sub-VLAN.</td>
<td>vlan vlan-id-list</td>
</tr>
</tbody>
</table>

Configuring a super VLAN

When you configure a super VLAN, follow these restrictions and guidelines:

- Do not configure the VLAN of a MAC address-to-VLAN entry as a super VLAN.
- Do not configure a VLAN as both a super VLAN and a guest VLAN, Auth-Fail VLAN, or critical VLAN. 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 sub-VLAN.
- Layer 2 multicast configuration for super VLANs does not take effect because they do not have physical ports.
To configure a super VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the VLAN as a super VLAN.</td>
<td>supervlan</td>
</tr>
<tr>
<td>4.</td>
<td>Associate the super VLAN with the sub-VLANs.</td>
<td>subvlan vlan-id-list</td>
</tr>
</tbody>
</table>

### Configuring a super VLAN interface

As a best practice, do not configure VRRP for a super VLAN interface because the configuration affects network performance. For more information about VRRP, see [High Availability Configuration Guide](#).

To configure a VLAN interface for a super VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VLAN interface and enter its view.</td>
<td>interface vlan-interface interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an IP address for the super VLAN interface.</td>
<td>• Configure an IPv4 address: ip address ip-address ( mask-length</td>
</tr>
<tr>
<td>4.</td>
<td>Configure Layer 3 communication between sub-VLANs.</td>
<td>• Enable local proxy ARP for devices that run IPv4 protocols: local-proxy-arp enable &lt;br&gt; • Enable local proxy ND for devices that run IPv6 protocols: local-proxy-nd enable</td>
</tr>
</tbody>
</table>

### Displaying and maintaining super VLANs

Execute `display` commands in any view.
Super VLAN configuration example

Network requirements

As shown in Figure 63:

- Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are in VLAN 2.
- Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 are in VLAN 3.
- Ten-GigabitEthernet 1/0/5 and Ten-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 63 Network diagram**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about super VLANs and their associated sub-VLANS.</td>
<td><code>display supervlan [ supervlan-id ]</code></td>
</tr>
</tbody>
</table>

Configuration procedure

# Create VLAN 10.
```bash
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

# Create VLAN-interface 10, and assign IP address 10.1.1.1/24 to it.
```bash
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
```

# Enable local proxy ARP.
```bash
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

# Create VLAN 2, and assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to the VLAN.
```bash
[DeviceA] vlan 2
[DeviceA-vlan2] port ten-gigabitethernet 1/0/1 ten-gigabitethernet 1/0/2
```
# Create VLAN 3, and assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to the VLAN.
[DeviceA] vlan 3
[DeviceA-vlan3] port ten-gigabitethernet 1/0/3 ten-gigabitethernet 1/0/4
[DeviceA-vlan3] quit

# Create VLAN 5, and assign Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 to the VLAN.
[DeviceA] vlan 5
[DeviceA-vlan5] port ten-gigabitethernet 1/0/5 ten-gigabitethernet 1/0/6
[DeviceA-vlan5] quit

# Configure VLAN 10 as a super VLAN, and associate sub-VLANs 2, 3, and 5 with the super VLAN.
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] subvlan 2 3 5
[DeviceA-vlan10] quit
[DeviceA] quit

Verifying the configuration

# Display information about super VLAN 10 and its associated sub-VLANs.
<DeviceA> display supervlan
Super VLAN ID: 10
Sub-VLAN ID: 2-3 5

VLAN ID: 10
VLAN type: Static
It is a super VLAN.
Route interface: Configured
Ipv4 address: 10.1.1.1
Ipv4 subnet mask: 255.255.255.0
Description: VLAN 0010
Name: VLAN 0010
Tagged ports: None
Untagged ports: None

VLAN ID: 2
VLAN type: Static
It is a sub VLAN.
Route interface: Configured
Ipv4 address: 10.1.1.1
Ipv4 subnet mask: 255.255.255.0
Description: VLAN 0002
Name: VLAN 0002
Tagged ports: None
Untagged ports:
  Ten-GigabitEthernet1/0/1
  Ten-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:
  Ten-GigabitEthernet1/0/3
  Ten-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:
  Ten-GigabitEthernet1/0/5
  Ten-GigabitEthernet1/0/6
Configuring the private VLAN

VLAN technology provides a method for isolating traffic from customers. At the access layer of a network, customer traffic must be isolated for security or accounting purposes. If VLANs are assigned on a per-user basis, a large number of VLANs will be required.

The private VLAN feature saves VLAN resources. It uses a two-tier VLAN structure as follows:

- **Primary VLAN**—Used for connecting the upstream device. A primary VLAN can be associated with multiple secondary VLANs. The upstream device identifies only the primary VLAN.
- **Secondary VLANs**—Used for connecting users. Secondary VLANs are isolated at Layer 2. To implement Layer 3 communication between secondary VLANs associated with the primary VLAN, enable local proxy ARP or ND on the upstream device (for example, L3 Device A in Figure 64).

As shown in Figure 64, the private VLAN feature is enabled on L2 Device B. VLAN 10 is the primary VLAN. VLANs 2, 5, and 8 are secondary VLANs that are associated with VLAN 10. L3 Device A is only aware of VLAN 10.

**Figure 64 Private VLAN example**

If the private VLAN feature is configured on a Layer 3 device, use one of the following methods on the Layer 3 device to enable Layer 3 communication. Layer 3 communication might be required between secondary VLANs that are associated with the same primary VLAN, or between secondary VLANs and other networks.

- **Method 1:**
  a. Create VLAN interfaces for the secondary VLANs.
  b. Assign IP addresses to the secondary VLAN interfaces.
- **Method 2:**
  c. Enable Layer 3 communication between the secondary VLANs that are associated with the primary VLAN.
  d. Create the VLAN interface for the primary VLAN and assign an IP address to it. (Do not create secondary VLAN interfaces if you use this method.)
  e. Enable local proxy ARP or ND on the primary VLAN interface.

**Configuration task list**

To configure the private VLAN feature, perform the following tasks:

1. Configure the primary VLAN.
2. Configure the secondary VLANs.
3. Associate the secondary VLANs with the primary VLAN.

4. Configure the uplink and downlink ports:
   - Configure the uplink port (for example, the port connecting L2 Device B to L3 Device A in Figure 64):
     - 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 the primary VLANs and their associated secondary VLANs.
   - Configure a downlink port (for example, the port connecting L2 Device B to a host in Figure 64) as a host port. The host port can be automatically assigned to the secondary VLAN and its associated primary VLAN.
   - If a downlink port allows multiple secondary VLANs, configure the port as a trunk secondary port. The trunk secondary port can be automatically assigned to the secondary VLANs and their associated primary VLANs.

For more information about promiscuous, trunk promiscuous, host, and trunk secondary ports, see Layer 2—LAN Switching Command Reference.

5. 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:

- Make sure the following requirements are met:
  - For a promiscuous port:
    - 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:
    - The PVID of the port is a secondary VLAN.
    - The port is an untagged member of the primary VLAN and the secondary VLAN.
  - A trunk promiscuous or trunk secondary port must be 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VLAN and</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>enter VLAN view.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the VLAN</td>
<td>private-vlan</td>
</tr>
<tr>
<td></td>
<td>as a primary VLAN.</td>
<td>primary</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Create one or</td>
<td>vlan { vlan-id-list</td>
</tr>
<tr>
<td></td>
<td>multiple</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>secondary VLANs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>7.</td>
<td>Enter VLAN view of the primary VLAN.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>8.</td>
<td>Associate the primary VLAN with the secondary VLANs.</td>
<td>private-vlan secondary vlan-id-list</td>
</tr>
<tr>
<td>9.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>10.</td>
<td>Enter interface view of the uplink port.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>11.</td>
<td>Configure the uplink port as a promiscuous or trunk promiscuous port of the specified VLANs.</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>13.</td>
<td>Enter interface view of the downlink port.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>14.</td>
<td>Assign the downlink port to secondary VLANs.</td>
<td>a Set the link type of the port: port link-type { access</td>
</tr>
<tr>
<td>15.</td>
<td>Configure the downlink port as a host or trunk secondary port.</td>
<td>• Configure the downlink port as a host port: port private-vlan host • Configure the downlink port as a trunk secondary port of the specified VLANs: port private-vlan vlan-id-list trunk secondary</td>
</tr>
<tr>
<td>16.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>17.</td>
<td>Enter VLAN view of a secondary VLAN.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>18.</td>
<td>(Optional.) Enable Layer 2 communication for ports in the same secondary VLAN.</td>
<td>• undo private-vlan isolated • private-vlan community</td>
</tr>
<tr>
<td>19.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
</tbody>
</table>
20. (Optional.) Configure Layer 3 communication between the specified secondary VLANs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Enter VLAN interface view of the primary VLAN interface: interface vlan-interface interface-number</td>
<td>Use substeps a, b, c, and e for devices that run IPv4 protocols. Use substeps a, b, d, and f for devices that run IPv6 protocols. By default: • Secondary VLANs cannot communicate with each other at Layer 3. • No IP address is configured for a VLAN interface. • Local proxy ARP and ND are disabled. For more information about local proxy ARP and ND, see Layer 3—IP Services Configuration Guide. For more information about the local-proxy-arp enable and local-proxy-nd enable commands, see Layer 3—IP Services Command Reference.</td>
</tr>
<tr>
<td>b</td>
<td>Enable Layer 3 communication between secondary VLANs that are associated with the primary VLAN: private-vlan secondary vlan-id-list</td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>Assign an IPv4 address to the primary VLAN interface: ip address ip-address { mask-length</td>
<td>mask } [ sub ]</td>
</tr>
<tr>
<td>d</td>
<td>Assign an IPv6 address to the primary VLAN interface: ipv6 address { ipv6-address prefix-length</td>
<td>ipv6-address/prefix-length }</td>
</tr>
<tr>
<td>e</td>
<td>Enable local proxy ARP: local-proxy-arp enable</td>
<td></td>
</tr>
<tr>
<td>f</td>
<td>Enable local proxy ND: local-proxy-nd enable</td>
<td></td>
</tr>
</tbody>
</table>

Displaying and maintaining the private VLAN

Execute display commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about primary VLANs and the secondary VLANs associated with each primary VLAN.</td>
<td>display private-vlan [ primary-vlan-id ]</td>
</tr>
</tbody>
</table>

Private VLAN configuration examples

Promiscuous port configuration example

Network requirements

As shown in Figure 65, 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. Ten-GigabitEthernet 1/0/5 is in VLAN 5. Ten-GigabitEthernet 1/0/2 is in VLAN 2. Ten-GigabitEthernet 1/0/3 is in VLAN 3.
- On Device C, VLAN 6 is a primary VLAN that is associated with secondary VLANs 3 and 4. Ten-GigabitEthernet 1/0/5 is in VLAN 6. Ten-GigabitEthernet 1/0/3 is in VLAN 3. Ten-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.
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
   
   # Associate secondary VLANs 2 and 3 with primary VLAN 5.
   [DeviceB] vlan 5
   [DeviceB-vlan5] private-vlan secondary 2 to 3
   [DeviceB-vlan5] quit
   
   # Configure the uplink port (Ten-GigabitEthernet 1/0/5) as a promiscuous port of VLAN 5.
   [DeviceB] interface ten-gigabitethernet 1/0/5
   [DeviceB-Ten-GigabitEthernet1/0/5] port private-vlan 5 promiscuous
   [DeviceB-Ten-GigabitEthernet1/0/5] quit
   
   # Assign downlink port Ten-GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.
   [DeviceB] interface ten-gigabitethernet 1/0/2
   [DeviceB-Ten-GigabitEthernet1/0/2] port access vlan 2
   [DeviceB-Ten-GigabitEthernet1/0/2] port private-vlan host
   [DeviceB-Ten-GigabitEthernet1/0/2] quit
   
   # Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.
   [DeviceB] interface ten-gigabitethernet 1/0/3
   [DeviceB-Ten-GigabitEthernet1/0/3] port access vlan 3
   [DeviceB-Ten-GigabitEthernet1/0/3] port private-vlan host
   ```
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

   # Associate secondary VLANs 3 and 4 with primary VLAN 6.
   [DeviceC] vlan 6
   [DeviceC-vlan6] private-vlan secondary 3 to 4
   [DeviceC-vlan6] quit

   # Configure the uplink port (Ten-GigabitEthernet 1/0/5) as a promiscuous port of VLAN 6.
   [DeviceC] interface ten-gigabitethernet 1/0/5
   [DeviceC-Ten-GigabitEthernet1/0/5] port private-vlan 6 promiscuous
   [DeviceC-Ten-GigabitEthernet1/0/5] quit

   # Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.
   [DeviceC] interface ten-gigabitethernet 1/0/3
   [DeviceC-Ten-GigabitEthernet1/0/3] port access vlan 3
   [DeviceC-Ten-GigabitEthernet1/0/3] port private-vlan host
   [DeviceC-Ten-GigabitEthernet1/0/3] quit

   # Assign downlink port Ten-GigabitEthernet 1/0/4 to VLAN 4, and configure the port as a host port.
   [DeviceC] interface ten-gigabitethernet 1/0/4
   [DeviceC-Ten-GigabitEthernet1/0/4] port access vlan 4
   [DeviceC-Ten-GigabitEthernet1/0/4] port private-vlan host
   [DeviceC-Ten-GigabitEthernet1/0/4] quit

Verifying the configuration
   # Verify the private VLAN configurations 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:
   - Ten-GigabitEthernet1/0/2
   - Ten-GigabitEthernet1/0/3
   - Ten-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:
    Ten-GigabitEthernet1/0/2
    Ten-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:
    Ten-GigabitEthernet1/0/3
    Ten-GigabitEthernet1/0/5

The output shows that:
1. The promiscuous port (Ten-GigabitEthernet 1/0/5) is an untagged member of primary VLAN 5 and secondary VLANs 2 and 3.
2. Host port Ten-GigabitEthernet 1/0/2 is an untagged member of primary VLAN 5 and secondary VLAN 2.
3. Host port Ten-GigabitEthernet 1/0/3 is an untagged member of primary VLAN 5 and secondary VLAN 3.

Trunk promiscuous port configuration example

Network requirements

As shown in Figure 66, configure the private VLAN feature to meet the following requirements:
1. VLANs 5 and 10 are primary VLANs on Device B. The uplink port (Ten-GigabitEthernet 1/0/1) on Device B permits the packets from VLANs 5 and 10 to pass through tagged.
4. Device A is aware of only VLANs 5 and 10 on Device B.
1. Configure Device B:

   # Configure VLANs 5 and 10 as primary VLANs.
   <DeviceB> system-view
   [DeviceB] vlan 5
   [DeviceB-vlan5] private-vlan primary
   [DeviceB-vlan5] quit
   [DeviceB] vlan 10
   [DeviceB-vlan10] private-vlan primary
   [DeviceB-vlan10] quit

   # Create VLANs 2, 3, 6, and 8.
   [DeviceB] vlan 2 to 3
   [DeviceB] vlan 6
   [DeviceB-vlan6] quit
   [DeviceB] vlan 8
   [DeviceB-vlan8] quit

   # Associate secondary VLANs 2 and 3 with primary VLAN 5.
   [DeviceB] vlan 5
   [DeviceB-vlan5] private-vlan secondary 2 to 3
   [DeviceB-vlan5] quit

   # Associate secondary VLANs 6 and 8 with primary VLAN 10.
   [DeviceB] vlan 10
   [DeviceB-vlan10] private-vlan secondary 6 8
   [DeviceB-vlan10] quit

   # Configure the uplink port (Ten-GigabitEthernet 1/0/1) as a trunk promiscuous port of VLANs 5 and 10.
   [DeviceB] interface ten-gigabitethernet 1/0/1
   [DeviceB-Ten-GigabitEthernet1/0/1] port private-vlan 5 10 trunk promiscuous
   [DeviceB-Ten-GigabitEthernet1/0/1] quit
# Assign downlink port Ten-GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-Ten-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/2] quit

# Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/3] quit

# Assign downlink port Ten-GigabitEthernet 1/0/4 to VLAN 6, and configure the port as a host port.
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port access vlan 6
[DeviceB-Ten-GigabitEthernet1/0/4] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/4] quit

# Assign downlink port Ten-GigabitEthernet 1/0/5 to VLAN 8, and configure the port as a host port.
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port access vlan 8
[DeviceB-Ten-GigabitEthernet1/0/5] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/5] quit

2. Configure Device A:

# Create VLANs 5 and 10.
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit

# Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 5 and 10 as a tagged VLAN member.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-Ten-GigabitEthernet1/0/1] quit

Verifying the configuration

# Verify the 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:
  - Ten-GigabitEthernet1/0/1
Untagged ports:
  - Ten-GigabitEthernet1/0/2
  - Ten-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:
  - Ten-GigabitEthernet1/0/1
Untagged ports:
  - Ten-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:
  - Ten-GigabitEthernet1/0/1
Untagged ports:
  - Ten-GigabitEthernet1/0/3

The output shows that:
- The trunk promiscuous port (Ten-GigabitEthernet 1/0/1) is a tagged member of primary VLAN 5 and secondary VLANs 2 and 3.
- Host port Ten-GigabitEthernet 1/0/2 is an untagged member of primary VLAN 5 and secondary VLAN 2.
- Host port Ten-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 67, configure the private VLAN feature to meet the following requirements:
- VLANs 10 and 20 are primary VLANs on Device A. The uplink port (Ten-GigabitEthernet 1/0/5) on Device A permits the packets from VLANs 10 and 20 to pass through tagged.
- VLANs 11, 12, 21, and 22 are secondary VLANs on Device A.
  - Downlink port Ten-GigabitEthernet 1/0/2 permits the packets from secondary VLANs 11 and 21 to pass through tagged.
  - Downlink port Ten-GigabitEthernet 1/0/1 permits secondary VLAN 22.
• Downlink port Ten-GigabitEthernet 1/0/3 permits secondary 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 67 Network diagram**

![Network Diagram]

**Configuration procedure**

1. Configure Device A:

   # Configure VLANs 10 and 20 as primary VLANs.
   
   ```
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] private-vlan primary
   [DeviceA-vlan10] quit
   [DeviceA] vlan 20
   [DeviceA-vlan20] private-vlan primary
   [DeviceA-vlan20] quit
   # Create VLANs 11, 12, 21, and 22.
   [DeviceA] vlan 11 to 12
   [DeviceA] vlan 21 to 22
   # Associate secondary VLANs 11 and 12 with primary VLAN 10.
   [DeviceA] vlan 10
   [DeviceA-vlan10] private-vlan secondary 11 12
   [DeviceA-vlan10] quit
   # Associate secondary VLANs 21 and 22 with primary VLAN 20.
   [DeviceA] vlan 20
   [DeviceA-vlan20] private-vlan secondary 21 22
   ```
# Configure the uplink port (Ten-GigabitEthernet 1/0/5) as a trunk promiscuous port of VLANs 10 and 20.
[DeviceA] interface ten-gigabitethernet 1/0/5
[DeviceA-Ten-GigabitEthernet1/0/5] port private-vlan 10 20 trunk promiscuous
[DeviceA-Ten-GigabitEthernet1/0/5] quit

# Assign downlink port Ten-GigabitEthernet 1/0/1 to VLAN 22 and configure the port as a host port.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port access vlan 22
[DeviceA-Ten-GigabitEthernet1/0/1] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/1] quit

# Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 12 and configure the port as a host port.
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port access vlan 12
[DeviceA-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/3] quit

# Configure downlink port Ten-GigabitEthernet 1/0/2 as a trunk secondary port of VLANs 11 and 21.
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port private-vlan 11 21 trunk secondary
[DeviceA-Ten-GigabitEthernet1/0/2] quit

2. Configure Device B:

# Create VLANs 11 and 21.
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit

# Configure Ten-GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLANs 11 and 21 as a tagged VLAN member.
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type hybrid
[DeviceB-Ten-GigabitEthernet1/0/2] port hybrid vlan 11 21 tagged
[DeviceB-Ten-GigabitEthernet1/0/2] quit

# Assign Ten-GigabitEthernet 1/0/3 to VLAN 11.
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port access vlan 11
[DeviceB-Ten-GigabitEthernet1/0/3] quit

# Assign Ten-GigabitEthernet 1/0/4 to VLAN 21.
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port access vlan 21
[DeviceB-Ten-GigabitEthernet1/0/4] quit

3. Configure Device C:

# Create VLANs 10 and 20.
<DeviceC> system-view
[DeviceC] vlan 10
# Configure Ten-GigabitEthernet 1/0/5 as a hybrid port, and assign it to VLANs 10 and 20 as a tagged VLAN member.

[DeviceC] interface ten-gigabitethernet 1/0/5
[DeviceC-Ten-GigabitEthernet1/0/5] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/5] port hybrid vlan 10 20 tagged
[DeviceC-Ten-GigabitEthernet1/0/5] quit

Verifying the configuration

# Verify the primary VLAN configurations on Device A. The following output uses primary VLAN 10 as an example.

[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:
- Ten-GigabitEthernet1/0/2
- Ten-GigabitEthernet1/0/5
Untagged ports:
- Ten-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:
- Ten-GigabitEthernet1/0/2
- Ten-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:
- Ten-GigabitEthernet1/0/5
Untagged ports:
The output shows that:

- The trunk promiscuous port (Ten-GigabitEthernet 1/0/5) is a tagged member of primary VLAN 10 and secondary VLANs 11 and 12.
- The trunk secondary port (Ten-GigabitEthernet 1/0/2) is a tagged member of primary VLAN 10 and secondary VLAN 11.
- The host port (Ten-GigabitEthernet 1/0/3) is an untagged member of primary VLAN 10 and secondary VLAN 12.

Secondary VLAN Layer 3 communication configuration example

Network requirements

As shown in Figure 68, configure the private VLAN feature to meet the following requirements:

- Primary VLAN 10 on Device A is associated with secondary VLANs 2 and 3. The IP address of VLAN-interface 10 is 192.168.1.1/24.
- Ten-GigabitEthernet 1/0/1 belongs to VLAN 10. Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 belong to VLAN 2 and VLAN 3, respectively.
- Secondary VLANs are isolated at Layer 2 but interoperable at Layer 3.

Figure 68 Network diagram

Configuration procedure

# Create VLAN 10 and configure it as a primary VLAN.
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit

# Create VLANs 2 and 3.
<DeviceA> system-view
[DeviceA] vlan 2 to 3

# Associate primary VLAN 10 with secondary VLANs 2 and 3.
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] private-vlan secondary 2 3
[DeviceA-vlan10] quit
# Configure the uplink port (Ten-GigabitEthernet 1/0/1) as a promiscuous port of VLAN 10.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceA-Ten-GigabitEthernet1/0/1] quit

# Assign downlink port Ten-GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port access vlan 2
[DeviceA-Ten-GigabitEthernet1/0/2] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/2] quit

# Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port access vlan 3
[DeviceA-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/3] quit

# Enable Layer 3 communication between secondary VLANs 2 and 3 that are associated with primary VLAN 10.
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] private-vlan secondary 2 3

# Assign IP address 192.168.1.1/24 to VLAN-interface 10.
[DeviceA-Vlan-interface10] ip address 192.168.1.1 255.255.255.0

# Enable local proxy ARP on VLAN-interface 10.
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit

Verifying the configuration

# Display the configuration of primary VLAN 10.
[DeviceA] 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:
  Ten-GigabitEthernet1/0/1
  Ten-GigabitEthernet1/0/2
  Ten-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:
   Ten-GigabitEthernet1/0/1
   Ten-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:
   Ten-GigabitEthernet1/0/1
   Ten-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. The device can configure QoS parameters for voice packets to ensure higher transmission priority of the voice packets.

Common voice devices include IP phones and integrated access devices (IADs). This chapter uses IP phones as an example.

For an IP phone to access a device, the device must perform the following operations:
1. Identify the IP phone in the network and obtain the MAC address of the IP phone.
2. Advertise the voice VLAN information to the IP phone.

After receiving the voice VLAN information, the IP phone performs automatic configuration. Voice packets sent from the IP phone can then 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 identifies voice packets based on their source MAC addresses. A packet whose source MAC address complies with an Organizationally Unique Identifier (OUI) address of the device is regarded as a voice packet.

You can use system default OUI addresses (see Table 14) or configure OUI addresses for the device. You can manually remove or add the system default OUI addresses.

Table 14 Default OUI addresses

<table>
<thead>
<tr>
<th>Number</th>
<th>OUI address</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0001-e300-0000</td>
<td>Siemens phone</td>
</tr>
<tr>
<td>2</td>
<td>0003-6b00-0000</td>
<td>Cisco phone</td>
</tr>
<tr>
<td>3</td>
<td>0004-0d00-0000</td>
<td>Avaya phone</td>
</tr>
<tr>
<td>4</td>
<td>000f-e200-0000</td>
<td>H3C Aolynk phone</td>
</tr>
<tr>
<td>5</td>
<td>0060-b900-0000</td>
<td>Philips/NEC phone</td>
</tr>
<tr>
<td>6</td>
<td>00d0-1e00-0000</td>
<td>Pingtel phone</td>
</tr>
<tr>
<td>7</td>
<td>00e0-7500-0000</td>
<td>Polycom phone</td>
</tr>
<tr>
<td>8</td>
<td>00e0-bb00-0000</td>
<td>3Com phone</td>
</tr>
</tbody>
</table>

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 identify voice packets. They are the logical AND results of the mac-address and oui-mask arguments in the voice-vlan mac-address command.
Automatically identifying IP phones through LLDP

If IP phones support LLDP, configure LLDP for automatic IP phone discovery on the device. The device can then 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 performs the following operations:
1. Sends an LLDP TLV with the voice VLAN configuration to the peer.
2. Assigns the receiving port to the voice VLAN.
3. Increases the transmission priority of the voice packets sent from the IP phone.
4. Adds the MAC address of the IP phone to the MAC address table to ensure that the IP phone can pass authentication.

Use LLDP instead of the OUI list to identify IP phones if the network has more IP phone categories than the maximum number of OUI addresses supported on the device. LLDP has higher priority than the OUI list.

For more information about LLDP, see "Configuring LLDP."

Advertising the voice VLAN information to IP phones

Figure 69 shows the workflow of advertising the voice VLAN information to IP phones.

Figure 69 Workflow of advertising the voice VLAN information to IP phones

IP phone access methods

Connecting the host and the IP phone in series

As shown in Figure 70, 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.
Connecting the IP phone to the device

As shown in Figure 71, IP phones are connected to the device without the presence of the host. Use this connection method when IP phones send out untagged voice packets. In this scenario, you must configure the voice VLAN as the PVID of the access port of the IP phone, and configure the port to forward the packets from the PVID.

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 70. Ports on the device transmit both voice traffic and data traffic.

When an IP phone is powered on, it sends out protocol packets. After receiving these protocol packets, the device uses the source MAC address of the protocol packets to match its OUI addresses. If the match succeeds, the device performs the following operations:

• Assigns the receiving port of the protocol packets to the voice VLAN.
• Issues ACL rules to set the packet precedence.
• Starts the voice VLAN aging timer.

If no voice packet is received from the port before the aging timer expires, the device will remove the port from the voice VLAN. The aging timer is also configurable.
When the IP phone reboots, the port is reassigned to the voice VLAN to ensure the correct operation of the existing voice connections. The reassignment occurs automatically without being triggered by voice traffic as long as the voice VLAN operates correctly.

**Manual mode**

Use manual mode when only IP phones access the network through the device, as shown in Figure 71. In this mode, ports are assigned to a voice VLAN that transmits voice traffic exclusively. No data traffic affects the voice traffic transmission.

You must manually assign the port that connects to the IP phone to a voice VLAN. The device uses the source MAC address of the received voice packets to match its OUI addresses. If the match succeeds, the device issues ACL rules to set the packet precedence.

To remove the port from the voice VLAN, you must manually remove it.

**Cooperation of voice VLAN assignment modes and IP phones**

Some IP phones send out VLAN-tagged packets, and others send out only untagged packets. For correct packet processing, ports of different link types must meet specific configuration requirements in different voice VLAN assignment modes.

Access ports do not transmit tagged packets.

**Table 15 Configuration requirements for trunk and hybrid ports to support tagged voice traffic**

<table>
<thead>
<tr>
<th>Port link type</th>
<th>Voice VLAN assignment mode</th>
<th>Configuration requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trunk</td>
<td>Automatic</td>
<td>The PVID of the port cannot be the voice VLAN.</td>
</tr>
<tr>
<td></td>
<td>Manual</td>
<td>The PVID of the port cannot be the voice VLAN. The port must forward packets from the voice VLAN.</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Automatic</td>
<td>The PVID of the port cannot be the voice VLAN.</td>
</tr>
<tr>
<td></td>
<td>Manual</td>
<td>The PVID of the port cannot be the voice VLAN. The port must forward packets from the voice VLAN with VLAN tags.</td>
</tr>
</tbody>
</table>

When IP phones send out untagged packets, you must set the voice VLAN assignment mode to manual.

**Table 16 Configuration requirements for ports in manual mode to support untagged voice traffic**

<table>
<thead>
<tr>
<th>Port link type</th>
<th>Configuration requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>The voice VLAN must be the PVID of the port.</td>
</tr>
<tr>
<td>Trunk</td>
<td>The voice VLAN must be the PVID of the port. The port must forward packets from the voice VLAN.</td>
</tr>
<tr>
<td>Hybrid</td>
<td>The voice VLAN must be the PVID of the port. The port must forward packets from the voice VLAN without VLAN tags.</td>
</tr>
</tbody>
</table>
If an IP phone sends out tagged voice traffic, and its access port is configured with 802.1X authentication, guest VLAN, Auth-Fail VLAN, or critical VLAN, VLAN IDs must be different for the following VLANs:

- Voice VLAN.
- PVID of the access port.
- 802.1X guest, Auth-Fail, or critical VLAN.

If an IP phone sends out untagged voice traffic, the PVID of the access port must be the voice VLAN. In this scenario, 802.1X authentication is not supported.

## Security mode and normal mode of voice VLANs

Depending on the filtering mechanisms to incoming packets, 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 a large number of forged voice-VLAN-tagged or untagged packets to affect voice communication.

- **Security mode**—The port uses the source MAC addresses of voice packets to match the OUI addresses of the device. Packets that fail the match will be dropped.

In a safe network, you can configure the voice VLANs to operate in normal mode. This mode reduces system resource consumption in source MAC address checking.

In either mode, the device modifies the transmission priority only for voice VLAN packets whose source MAC addresses match OUI addresses of the device.

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 17 Packet processing on a voice VLAN-enabled port in normal or security mode

<table>
<thead>
<tr>
<th>Voice VLAN mode</th>
<th>Packet type</th>
<th>Packet processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Untagged packets, Packets with the voice VLAN tags</td>
<td>The port does not examine their source MAC addresses. Both voice traffic and non-voice traffic can be transmitted in the voice VLAN.</td>
</tr>
<tr>
<td></td>
<td>Packets with other VLAN tags</td>
<td>The port forwards or drops them depending on whether the port permits packets from these VLANs to pass through.</td>
</tr>
<tr>
<td>Security</td>
<td>Untagged packets, Packets with the voice VLAN tags</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Packets with other VLAN tags</td>
<td>The port forwards or drops them depending on whether the port permits packets from these VLANs to pass through.</td>
</tr>
</tbody>
</table>
## Voice VLAN configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring the QoS priority settings for voice traffic</td>
<td></td>
</tr>
<tr>
<td>(Required.) Use one of the following methods:</td>
<td></td>
</tr>
<tr>
<td>• Configuring a port to operate in automatic voice VLAN assignment mode</td>
<td></td>
</tr>
<tr>
<td>• Configuring a port to operate in manual voice VLAN assignment mode</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Enabling LLDP for automatic IP phone discovery</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Use one of the following methods:</td>
<td></td>
</tr>
<tr>
<td>• Configuring LLDP to advertise a voice VLAN</td>
<td></td>
</tr>
<tr>
<td>• Configuring CDP to advertise a voice VLAN</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the QoS priority settings for voice traffic

The QoS priority settings carried in voice traffic include the CoS and DSCP values. You can configure the device to modify the QoS priority settings for voice traffic.

You cannot configure the QoS priority settings on a voice VLAN-enabled port. Before you configure the QoS priority settings for voice traffic on a port, you must disable the voice VLAN feature on it.

To configure the QoS priority settings for voice traffic:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view. | • Enter Layer 2 Ethernet interface view: interface interface-type interface-number  
• Enter S-channel interface view: interface s-channel interface-number.channel-id  
• Enter S-channel aggregate interface view: interface schannel-aggregation interface-number:channel-id | N/A |
| 3.   | Configure QoS priority settings for incoming voice VLAN packets. | • 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 cos-value dscp-value | By default, a port modifies the CoS and DSCP values for voice VLAN packets to 6 and 46, respectively.  
If a port trusts the QoS priority settings in incoming voice VLAN packets, the port does not modify their CoS and DSCP values. |
Configuring a port to operate in automatic voice VLAN assignment mode

Configuration restrictions and guidelines

When you configure a port to operate in automatic voice VLAN assignment mode, follow these restrictions and guidelines:

- Do not configure a VLAN as both a voice VLAN and a protocol-based VLAN.
  - A voice VLAN in automatic mode on a hybrid port processes only tagged incoming voice traffic.
  - A protocol-based VLAN on a hybrid port processes only untagged incoming packets. For more information about protocol-based VLANs, see "Configuring protocol-based VLANs."
- As a best practice, do not use this mode 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 port will not be dynamically assigned to the voice VLAN.
- As a best practice, do not use this mode with PVST. In PVST mode, if the target voice VLAN is not permitted on a port, the port is placed in blocked state. The port drops the received packets instead of delivering them to the CPU. As a result, the 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. They can have a negative impact on each other.

Configuration procedure

To configure a port to operate in automatic voice VLAN assignment mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set the voice VLAN aging timer.</td>
<td>voice-vlan aging minutes</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Enable the voice VLAN security mode.</td>
<td>voice-vlan security enable</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Add an OUI address for voice packet identification.</td>
<td>voice-vlan mac-address oui-mask [ description text ]</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Enter Layer 2 Ethernet interface view:
  - interface interface-type interface-number
- Enter S-channel interface view:
  - interface s-channel interface-number.channel-id
- Enter S-channel aggregate interface view:
  - interface schannel-aggregation

219
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 6.   | Configure the link type of the port. | • port link-type trunk  
• port link-type hybrid | N/A |
| 7.   | Configure the port to operate in automatic voice VLAN assignment mode. | voice-vlan mode auto | By default, the automatic voice VLAN assignment mode is enabled. |
| 8.   | Enable the voice VLAN feature on the port. | voice-vlan vlan-id enable | By default, the voice VLAN feature is enabled. Before you execute this command, make sure the specified VLAN already exists. |

### Configuring a port to operate in manual voice VLAN assignment mode

#### Configuration restrictions and guidelines

When you configure a port to operate in manual voice VLAN assignment mode, follow these restrictions and guidelines:

- You can configure different voice VLANs for different ports on the same device. Make sure the following requirements are met:
  - One port can be configured with only one voice VLAN.
  - Voice VLANs must be existing static VLANs.
- Do not enable voice VLAN on the member ports of a link aggregation group. For more information about link aggregation, see "Configuring Ethernet link aggregation."
- To make a voice VLAN take effect on a port operating in manual mode, you must manually assign the port to the voice VLAN.

#### Configuration procedure

To configure a port to operate in manual voice VLAN assignment mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Enable the voice VLAN security mode.</td>
<td>voice-vlan security enable</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Add an OUI address for voice packet identification.</td>
<td>voice-vlan mac-address oui-mask oui-mask [ description text ]</td>
</tr>
</tbody>
</table>
| 4.   | Enter interface view. | • Enter Layer 2 Ethernet interface view:  
interface interface-type interface-number  
• Enter S-channel interface view:  
interface s-channel | N/A |
### Enabling LLDP for automatic IP phone discovery

#### Configuration restrictions and guidelines

When you enable LLDP for automatic IP phone discovery, following these restrictions and guidelines:

- Before you enable this feature, enable LLDP both globally and on access ports.
- Use this feature only with the automatic voice VLAN assignment mode.
- Do not use this feature together with CDP compatibility.
- After you enable this feature on the device, each port of the device can be connected to a maximum of five IP phones.

#### Configuration procedure

To enable LLDP for automatic IP phone discovery:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable</td>
<td>voice-vlan track lldp</td>
<td>By default, this feature is disabled.</td>
</tr>
</tbody>
</table>
Configuring LLDP to advertise a voice VLAN

For IP phones that support LLDP, the device advertises the voice VLAN information to the IP phones through the LLDP-MED TLVs.

Before you configure this feature, enable LLDP both globally and on access ports.

To configure LLDP to advertise a voice VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an advertised voice VLAN ID.</td>
<td>lldp tlv-enable med-tlv network-policy vlan-id</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Display the voice VLAN advertised by LLDP.</td>
<td>display lldp local-information</td>
</tr>
</tbody>
</table>

Configuring CDP to advertise a voice VLAN

If an IP phone supports CDP but does not support LLDP, it will send out CDP packets to the device to request the voice VLAN ID. If the IP phone does not receive the voice VLAN ID within a time period, it will send out untagged packets. The device cannot differentiate untagged voice packets from other types of packets.

You can configure CDP compatibility on the device to enable it to perform the following operations:

- Receive and identify CDP packets from the IP phone.
- Send CDP packets to the IP phone. The voice VLAN information is carried in the CDP packets.

After receiving the advertised VLAN information, the IP phone performs automatic voice VLAN configuration. Packets from the IP phone will be transmitted in the dedicated voice VLAN.

LLDP packets sent from the device carry the priority information. CDP packets sent from the device do not carry the priority information.

Before you configure this feature, enable LLDP globally and on access ports.

To configure CDP to advertise a voice VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable CDP compatibility.</td>
<td>lldp compliance cdp</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Configure CDP-compatible LLDP to operate in TxRx mode.</td>
<td>lldp compliance admin-status cdp txrx</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5.</td>
<td>cdp voice-vlan vlan-id</td>
<td>By default, no advertised voice VLAN ID is configured. For more information about the command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
</tbody>
</table>

## Displaying and maintaining voice VLANs

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the voice VLAN state.</td>
<td>display voice-vlan state</td>
</tr>
<tr>
<td>Display OUI addresses on a device.</td>
<td>display voice-vlan mac-address</td>
</tr>
</tbody>
</table>

## Voice VLAN configuration examples

### Automatic voice VLAN assignment mode configuration example

#### Network requirements

As shown in Figure 72, 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 phone A and IP phone B, respectively.
- Configure Ten-GigabitEthernet 1/0/1 and Ten-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.
- Set an aging timer for voice VLANs.
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
   # Enable security mode for voice VLANs.
   [DeviceA] voice-vlan security enable
   # Add MAC addresses of IP phones A and B to the device with mask FFF-F000-0000.
   [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 Ten-GigabitEthernet 1/0/1:
   # Configure Ten-GigabitEthernet 1/0/1 as a hybrid port.
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
   # Configure Ten-GigabitEthernet 1/0/1 to operate in automatic voice VLAN assignment mode.
   [DeviceA-Ten-GigabitEthernet1/0/1] voice-vlan mode auto
   # Enable voice VLAN on Ten-GigabitEthernet 1/0/1 and configure VLAN 2 as the voice VLAN for it.
   [DeviceA-Ten-GigabitEthernet1/0/1] voice-vlan 2 enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit

3. Configure Ten-GigabitEthernet 1/0/2:
   # Configure Ten-GigabitEthernet 1/0/2 as a hybrid port.
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-type hybrid
   # Configure Ten-GigabitEthernet 1/0/2 to operate in automatic voice VLAN assignment mode.
   [DeviceA-Ten-GigabitEthernet1/0/2] voice-vlan mode auto
   # Enable voice VLAN on Ten-GigabitEthernet 1/0/2 and configure VLAN 3 as the voice VLAN for it.
Verifying the configuration

# Display the OUI addresses supported on Device A.
[DeviceA] display voice-vlan mac-address

<table>
<thead>
<tr>
<th>OUI Address</th>
<th>Mask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-e300-0000</td>
<td>ffff-ff00-0000</td>
<td>Siemens phone</td>
</tr>
<tr>
<td>0003-6b00-0000</td>
<td>ffff-ff00-0000</td>
<td>Cisco phone</td>
</tr>
<tr>
<td>0004-0d00-0000</td>
<td>ffff-ff00-0000</td>
<td>Avaya phone</td>
</tr>
<tr>
<td>000f-e200-0000</td>
<td>ffff-ff00-0000</td>
<td>H3C Aolynk phone</td>
</tr>
<tr>
<td>0011-1100-0000</td>
<td>ffff-ff00-0000</td>
<td>IP phone A</td>
</tr>
<tr>
<td>0011-2200-0000</td>
<td>ffff-ff00-0000</td>
<td>IP phone B</td>
</tr>
<tr>
<td>0060-b900-0000</td>
<td>ffff-ff00-0000</td>
<td>Philips/NEC phone</td>
</tr>
<tr>
<td>00d0-1e00-0000</td>
<td>ffff-ff00-0000</td>
<td>Pingtel phone</td>
</tr>
<tr>
<td>00e0-7500-0000</td>
<td>ffff-ff00-0000</td>
<td>Polycom phone</td>
</tr>
<tr>
<td>00e0-bb00-0000</td>
<td>ffff-ff00-0000</td>
<td>3Com phone</td>
</tr>
</tbody>
</table>

# 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:

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
<th>Mode</th>
<th>CoS</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>2</td>
<td>Auto</td>
<td>6</td>
<td>46</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>3</td>
<td>Auto</td>
<td>6</td>
<td>46</td>
</tr>
</tbody>
</table>

Manual voice VLAN assignment mode configuration example

Network requirements

As shown in Figure 73, IP phone A send untagged voice traffic.

To enable Ten-GigabitEthernet 1/0/1 to transmit only voice packets, perform the following tasks on Device A:

- Create VLAN 2. This VLAN will be used as a voice VLAN.
- Configure Ten-GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode and add it to VLAN 2.
- Add the OUI address of IP phone A to the OUI list of Device A.
**Configuration procedure**

# Enable security mode for voice VLANs.
```
<DeviceA> system-view
[DeviceA] voice-vlan security enable
```

# Add MAC address 0011-2200-0001 with mask FFFF-FF00-0000.
```
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description test
```

# Create VLAN 2.
```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

# Configure Ten-GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.
```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

# Configure Ten-GigabitEthernet 1/0/1 as a hybrid port.
```
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
```

# Set the PVID of Ten-GigabitEthernet 1/0/1 to VLAN 2.
```
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 2
```

# Assign Ten-GigabitEthernet 1/0/1 to VLAN 2 as an untagged VLAN member.
```
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

# Enable voice VLAN and configure VLAN 2 as the voice VLAN on Ten-GigabitEthernet 1/0/1.
```
[DeviceA-Ten-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-Ten-GigabitEthernet1/0/1] quit
```

**Verifying the configuration**

# Display the OUI addresses supported on Device A.
```
[DeviceA] display voice-vlan mac-address
OUI Address    Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-2200-0001  ffff-ff00-0000  test
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```
# Display the voice VLAN state.

[DeviceA] display voice-vlan state
Current voice VLANs: 1
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled ports and their modes:

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
<th>Mode</th>
<th>CoS</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>2</td>
<td>Manual</td>
<td>6</td>
<td>46</td>
</tr>
</tbody>
</table>
Configuring MVRP

Multiple Registration Protocol (MRP) is an attribute registration protocol used to transmit attribute values. Multiple VLAN Registration Protocol (MVRP) is a typical MRP application. It synchronizes VLAN information among devices.

MVRP propagates local VLAN information to other devices, receives VLAN information from other devices, and dynamically updates local VLAN information. When the network topology changes, MVRP propagates and learns VLAN information again according to the new topology.

MRP

MRP allows devices in the same LAN to transmit attribute values on a per MSTI basis. For more information about MSTIs, see "Configuring spanning tree protocols."

MRP implementation

An MRP-enabled port is called an MRP participant. An MVRP-enabled port is called an MVRP participant.

As shown in Figure 74, an MRP participant sends declarations and withdrawals to notify other participants to register and deregister its attribute values. It also registers and deregisters the attribute values of other participants according to the received declarations and withdrawals. MRP rapidly propagates the configuration information of an MRP participant throughout the LAN.

Figure 74 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 74 shows a simple MRP implementation on an MSTI. In a network with multiple MSTIs, MRP performs attribute registration and deregistration on a per-MSTI basis.

MRP messages

MRP messages include the following types:

- Declaration—Includes Join and New messages.
- Withdrawal—Includes Leave and LeaveAll messages.
Join message

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

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

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

After receiving the Join message, other participants send the Join message to their respective peer participants.

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

- **JoinEmpty**—Declares an unregistered attribute. For example, when an MRP participant joins an unregistered static VLAN, it sends a JoinEmpty message. VLANs created manually and locally are called static VLANs. VLANs learned through MRP are called dynamic VLANs.

- **JoinIn**—Declares a registered attribute. A JoinIn message is used in one of the following situations:
  - An MRP participant joins an existing static VLAN and sends a JoinIn message after registering the VLAN.
  - The MRP participant receives a Join message propagated by another participant on the device and sends a JoinIn message after registering the VLAN.

New message

Similar to a Join message, a New message enables MRP participants to register attributes.

When the MSTP topology changes, an MRP participant sends a New message to the peer participant to declare the topology change.

Upon receiving a New message from the peer participant, an MRP participant performs the following tasks:

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

After receiving the New message, other participants send the New message to their respective peer participants.

Leave message

An MRP participant sends a Leave message to the peer participant when it wants the peer participant to deregister attributes that it has deregistered.

When the peer participant receives the Leave message, it performs the following tasks:

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

After a participant on the device receives the Leave message, it determines whether to send the Leave message to its peer participant depending on the attribute status on the device.

- If the VLAN in the Leave message is a dynamic VLAN not registered by any participants on the device, both of the following events occur:
  - The VLAN is deleted on the device.
  - The participant sends the Leave message to its peer participant.
- If the VLAN in the Leave message is a static VLAN, the participant will not send the Leave message to its peer participant.
LeaveAll message

Each MRP participant starts its LeaveAll timer when starting up. When the timer expires, the MRP participant sends LeaveAll messages to the peer participant.

Upon sending or receiving a LeaveAll message, the local participant starts the Leave timer. The local participant determines whether to send a Join message depending on its attribute status. A participant can re-register the attributes in the received Join message before the Leave timer expires.

When the Leave timer expires, a participant deregisters all attributes that have not been re-registered to periodically clear useless attributes in the network.

MRP timers

MRP uses the following timers to control message transmission.

Periodic timer

The Periodic timer controls the transmission of MRP messages. An MRP participant starts its own Periodic timer upon startup, and stores MRP messages to be sent before the Periodic timer expires. When the Periodic timer expires, MRP sends stored MRP messages in as few MRP frames as possible and restarts the Periodic timer. This mechanism reduces the number of MRP frames sent.

You can enable or disable the Periodic timer. When the Periodic timer is disabled, MRP does not periodically send MRP messages. Instead, an MRP participant sends MRP messages when the LeaveAll timer expires or the participant receives a LeaveAll message from the peer participant.

Join timer

The Join timer controls the transmission of Join messages. An MRP participant starts the Join timer after sending a Join message to the peer participant. Before the Join timer expires, the participant does not resend the Join message when the following conditions exist:

- The participant receives a JoinIn message from the peer participant.
- The received JoinIn message has the same attributes as the sent Join message.

When both the Join timer and the Periodic timer expire, the participant resends the Join message.

Leave timer

The Leave timer controls the deregistration of attributes.

An MRP participant starts the Leave timer in one of the following conditions:

- The participant receives a Leave message from its peer participant.
- The participant receives or sends a LeaveAll message.

The MRP participant does not deregister the attributes in the Leave or LeaveAll message if the following conditions exist:

- The participant receives a Join message before the Leave timer expires.
- The Join message includes the attributes that have been encapsulated in the Leave or LeaveAll message.

If the participant does not receive a Join message for these attributes before the Leave timer expires, MRP deregisters the attributes.

LeaveAll timer

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

Upon receiving the LeaveAll message, other participants restart their LeaveAll timer. The value of the LeaveAll timer is randomly selected between the LeaveAll timer and 1.5 times the LeaveAll timer. This mechanism provides the following benefits:
Effectively reduces the number of LeaveAll messages in the network.
Prevents the LeaveAll timer of a particular participant from always expiring first.

MVRP registration modes

VLAN information propagated by MVRP includes dynamic VLAN information from other devices and local static VLAN information.

MVRP has the following registration modes, which process dynamic VLANs in different ways.

Normal
An MVRP participant in normal registration mode registers and deregisters dynamic VLANs.

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

Forbidden
An MVRP participant in forbidden registration mode disables registering dynamic VLANs and drops received MVRP frames. The MVRP participant does not register new dynamic VLANs or re-register a deregistered dynamic VLAN.

Protocols and standards

IEEE 802.1ak, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks – Amendment 07: Multiple Registration Protocol

MVRP configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling MVRP</td>
</tr>
<tr>
<td>(Optional.) Setting an MVRP registration mode</td>
</tr>
<tr>
<td>(Optional.) Setting MRP timers</td>
</tr>
<tr>
<td>(Optional.) Enabling GVRP compatibility</td>
</tr>
</tbody>
</table>

Configuration restrictions and guidelines

When you configure MVRP, follow these restrictions and guidelines:

- MVRP can work with STP, RSTP, or MSTP. Ports blocked by STP, RSTP, or MSTP can receive and send MVRP frames. Do not configure MVRP with other link layer topology protocols, such as service loopback, PVST, RRPP, and Smart Link.
  - For more information about STP, RSTP, MSTP, and PVST, see "Configuring spanning tree protocols." For more information about service loopback, see "Configuring service loopback groups." For more information about RRPP and Smart Link, see High Availability Configuration Guide.
- Do not configure both MVRP and remote port mirroring on a port. Otherwise, MVRP might register the remote probe VLAN with incorrect ports, which would cause the monitor port to
receive undesired copies. For more information about port mirroring, see *Network Management and Monitoring Configuration Guide*.

- MVRP takes effect only on trunk ports. For more information about trunk ports, see "Configuring VLANs."
- Enabling MVRP on a Layer 2 aggregate interface takes effect on the aggregate interface and all Selected member ports in the link aggregation group.
- MVRP configuration made on an aggregation group member port takes effect only after the port is removed from the aggregation group.

### Configuration prerequisites

Before configuring MVRP, make sure each MSTI is mapped to an existing VLAN on each device in the network.

### Enabling MVRP

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable MVRP globally.</td>
<td>mvrp global enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, MVRP is globally disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For MVRP to take effect on a port, enable MVRP both on the port and globally.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the port as a trunk port.</td>
<td>port link-type trunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, each port is an access port. For more information about the port link-type trunk command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the trunk port to permit the specified VLANs.</td>
<td>port trunk permit vlan { vlan-id-list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a trunk port permits only VLAN 1. Make sure the trunk port permits all registered VLANs. For more information about the port trunk permit vlan command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
<tr>
<td>6.</td>
<td>Enable MVRP on the port.</td>
<td>mvrp enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, MVRP is disabled on a port.</td>
</tr>
</tbody>
</table>

### Setting an MVRP registration mode

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Setting MRP timers

To avoid frequent VLAN registrations and deregistrations, use the same MRP timers throughout the network.

Each port maintains its own Periodic, Join, and LeaveAll timers, and each attribute of a port maintains a Leave timer.

To set MRP timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>mrp timer leaveall timer-value</td>
<td>Optional. The default setting is 1000 centiseconds.</td>
</tr>
<tr>
<td>4.</td>
<td>mrp timer join timer-value</td>
<td>Optional. The default setting is 20 centiseconds.</td>
</tr>
<tr>
<td>5.</td>
<td>mrp timer leave timer-value</td>
<td>Optional. The default setting is 60 centiseconds.</td>
</tr>
<tr>
<td>6.</td>
<td>mrp timer periodic timer-value</td>
<td>Optional. The default setting is 100 centiseconds. You can restore the Periodic timer to the default at any time.</td>
</tr>
</tbody>
</table>

Table 18 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 18.
- As a best practice, restore the timers in the order of Join, Leave, and LeaveAll.

<table>
<thead>
<tr>
<th>Timer</th>
<th>Lower limit</th>
<th>Upper limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join</td>
<td>20 centiseconds</td>
<td>Half the Leave timer</td>
</tr>
<tr>
<td>Leave</td>
<td>Twice the Join timer</td>
<td>LeaveAll timer</td>
</tr>
<tr>
<td>LeaveAll</td>
<td>Leave timer on each port</td>
<td>32760 centiseconds</td>
</tr>
</tbody>
</table>
Enabling GVRP compatibility

Enable GVRP compatibility for MVRP when the peer device supports GVRP. Then, the local end can receive and send both MVRP and GVRP frames.

When you enable GVRP compatibility, follow these restrictions and guidelines:
- GVRP compatibility enables MVRP to work with STP or RSTP, but not MSTP.
- When the system is busy, disable the Period timer to prevent the participant from frequently registering or deregistering attributes.

For more information about GVRP, see the IEEE 802.1Q standard.

To enable GVRP compatibility:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>mvrp gvrp-compliance enable</td>
<td>By default, GVRP compatibility is disabled.</td>
</tr>
</tbody>
</table>

Displaying and maintaining MVRP

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display MVRP running status.</td>
<td><code>display mvrp running-status [ interface interface-list ]</code></td>
</tr>
<tr>
<td>Display the MVRP state of a port in a VLAN.</td>
<td><code>display mvrp state interface interface-type interface-number vlan vlan-id</code></td>
</tr>
<tr>
<td>Display MVRP statistics.</td>
<td><code>display mvrp statistics [ interface interface-list ]</code></td>
</tr>
<tr>
<td>Clear MVRP statistics.</td>
<td><code>reset mvrp statistics [ interface interface-list ]</code></td>
</tr>
</tbody>
</table>

MVRP configuration example

Network requirements

As shown in Figure 75:
- 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 configurations for each MSTI.
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 Ten-GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/1] port trunk permit vlan all
# Enable MVRP on port Ten-GigabitEthernet 1/0/1.
[DeviceA-Ten-GigabitEthernet1/0/1] mvrp enable
[DeviceA-Ten-GigabitEthernet1/0/1] quit
# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and configure it to permit VLAN 40.
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 40
# Enable MVRP on Ten-GigabitEthernet 1/0/2.
[DeviceA-Ten-GigabitEthernet1/0/2] mvrp enable
[DeviceA-Ten-GigabitEthernet1/0/2] quit
# Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/3] port trunk permit vlan all
# Enable MVRP on Ten-GigabitEthernet 1/0/3.
[DeviceA-Ten-GigabitEthernet1/0/3] mvrp enable
[DeviceA-Ten-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 Ten-GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-type trunk
# Enable MVRP on Ten-GigabitEthernet 1/0/1.
[DeviceB-Ten-GigabitEthernet1/0/1] mvrp enable
# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and configure it to permit all VLANs.
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/2] port trunk permit vlan all
# Enable MVRP on Ten-GigabitEthernet 1/0/2.
[DeviceB-Ten-GigabitEthernet1/0/2] mvrp enable
# Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/3] port trunk permit vlan all
# Enable MVRP on Ten-GigabitEthernet 1/0/3.
[DeviceB-Ten-GigabitEthernet1/0/3] mvrp enable

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 Ten-GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.
   [DeviceC] interface ten-gigabitethernet 1/0/1
   [DeviceC-Ten-GigabitEthernet1/0/1] port link-type trunk
   [DeviceC-Ten-GigabitEthernet1/0/1] port trunk permit vlan all
   # Enable MVRP on Ten-GigabitEthernet 1/0/1.
   [DeviceC-Ten-GigabitEthernet1/0/1] mvrp enable
   [DeviceC-Ten-GigabitEthernet1/0/1] quit
   # Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and configure it to permit all VLANs.
Configure Device C:

# Enable MVRP on Ten-GigabitEthernet 1/0/2.
[DeviceC-Ten-GigabitEthernet1/0/2] mvrp enable
[DeviceC-Ten-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 Ten-GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.
[DeviceD] interface ten-gigabitethernet 1/0/1
[DeviceD-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-Ten-GigabitEthernet1/0/1] port trunk permit vlan 20 40

# Enable MVRP on Ten-GigabitEthernet 1/0/1.
[DeviceD-Ten-GigabitEthernet1/0/1] mvrp enable
[DeviceD-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and configure it to permit VLAN 40.
[DeviceD] interface ten-gigabitethernet 1/0/2
[DeviceD-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-Ten-GigabitEthernet1/0/2] port trunk permit vlan 40

# Enable MVRP on Ten-GigabitEthernet 1/0/2.
[DeviceD-Ten-GigabitEthernet1/0/2] mvrp enable
[DeviceD-Ten-GigabitEthernet1/0/2] quit

Verifying the configuration

Verifying the normal registration mode configuration

# Display local VLAN information on Device A.
[DeviceA] display mvrp running-status
----------[MVRP Global Info]----------
Global Status : Enabled
Compliance-GVRP : False
### Ten-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)

### Ten-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

### Ten-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:

- Ten-GigabitEthernet 1/0/1 has registered VLAN 1, declared VLAN 1, VLAN 10, and VLAN 20, and propagated VLAN 1 through MVRP.
- Ten-GigabitEthernet 1/0/2 has declared VLAN 1, and registered and propagated no VLANs.
- Ten-GigabitEthernet 1/0/3 has registered VLAN 20, declared VLAN 1 and VLAN 10, and propagated VLAN 20 through MVRP.

# Display local VLAN information on Device B.

```
[DeviceB] display mvrp running-status
---------[MVRP Global Info]---------
Global Status : Enabled
Compliance-GVRP : False

----[Ten-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)

----[Ten-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)

----[Ten-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:

- Ten-GigabitEthernet 1/0/1 has registered VLAN 1, declared VLAN 1 and VLAN 20, and propagated VLAN 1 through MVRP.
- Ten-GigabitEthernet 1/0/2 has registered VLAN 1 and VLAN 10, declared VLAN 1 and VLAN 20, and propagated VLAN 1.
- Ten-GigabitEthernet 1/0/3 has registered VLAN 1 and VLAN 10, declared VLAN 20, and propagated VLAN 10 through MVRP.

# Display local VLAN information on Device C.
[DeviceC] display mvrp running-status

-------[MVRP Global Info]-------
Global Status     : Enabled
Compliance-GVRP   : False

----[Ten-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

----[Ten-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:
• Ten-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.
• Ten-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 local VLAN information on Device D.
[DeviceD] display mvrp running-status

-------[MVRP Global Info]-------
Global Status : Enabled
Compliance-GVRP : False

----[Ten-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

----[Ten-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:
• Ten-GigabitEthernet 1/0/1 has registered and propagated VLAN 10 and VLAN 20, and declared VLAN 1 through MVRP.
• Ten-GigabitEthernet 1/0/2 has registered VLAN 1, and declared and propagated no VLANs through MVRP.

Verifying the configuration after changing the registration mode

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

# Set the MVRP registration mode to fixed on Ten-GigabitEthernet 1/0/3 of Device B.
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] mvrp registration fixed
[DeviceB-Ten-GigabitEthernet1/0/3] quit

# Display local MVRP VLAN information on Ten-GigabitEthernet 1/0/3.
[DeviceB] display mvrp running-status interface ten-gigabitethernet 1/0/3

-------[MVRP Global Info]-------
Global Status     : Enabled
Compliance-GVRP   : False

----[Ten-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 Ten-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 local MVRP VLAN information on Ten-GigabitEthernet 1/0/3 of Device B.
[DeviceB] display mvrp running-status interface ten-gigabitethernet 1/0/3

-------[MVRP Global Info]-------
Global Status     : Enabled
Compliance-GVRP   : False

----[Ten-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 dynamic VLAN information on Ten-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 different 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 76, a QinQ frame transmitted over the service provider network carries the following tags:

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

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

![Figure 76 Single-tagged Ethernet frame header and double-tagged Ethernet frame header](image)

As shown in Figure 77, customer A has remote sites CE 1 and CE 4. Customer B has remote sites CE 2 and CE 3. The CVLANs of the two customers overlap. The service provider assigns SVLANs 3 and 4 to customers A and B, respectively.
When a tagged Ethernet frame from CE 1 arrives at PE 1, the PE tags the frame with SVLAN 3. The double-tagged Ethernet frame travels over the service provider network until it arrives at PE 2. PE 2 removes the SVLAN tag of the frame, and then sends the frame to CE 4.

**Figure 77 Typical QinQ application scenario**

QinQ implementations

QinQ is enabled on a per-port basis. The link type of a QinQ-enabled port can be access, hybrid, or trunk. The QinQ tagging behaviors are the same across these types of ports.

A QinQ-enabled port tags all incoming frames (tagged or untagged) with the PVID tag.

- If an incoming frame already has one tag, it becomes a double-tagged frame.
- If the frame does not have any 802.1Q tags, it becomes a frame tagged with the PVID.

QinQ provides the most basic VLAN manipulation method to tag all incoming frames (tagged or untagged) with the PVID tag. To perform advanced VLAN manipulations, use VLAN mappings or QoS policies as follows:

- To add different SVLANs for different CVLAN tags, use one-to-two VLAN mappings.
- To replace the SVLAN ID, CVLAN ID, or both IDs for an incoming double-tagged frame, use two-to-two VLAN mappings.
- QinQ and two-to-two mappings are mutually exclusive. The device does not support adding an SVLAN tag on a QinQ-enabled port and then modifying the CVLAN and SVLAN IDs.
- To use criteria other than the CVLAN ID to match packets for SVLAN tagging, use the QoS nest action. The QoS nest action can also be used with other actions in the same traffic behavior.
- To set the 802.1p priority in SVLAN tags, use the priority marking action as described in "Setting the 802.1p priority in SVLAN tags."

For more information about VLAN mappings, see "Configuring VLAN mapping." For more information about QoS, see *ACL and QoS Configuration Guide.*
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:

- 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 their forwarding path. This value is the sum of the default Ethernet interface MTU (1500 bytes) and the length (4 bytes) of a VLAN tag.
- You can use a VLAN mapping, a QoS policy, and QinQ on a port for VLAN tag manipulation. If their settings conflict, the configurations take effect based on their priorities in the following descending order: QoS policy > VLAN mapping > QinQ.

Enabling QinQ

Enable QinQ on customer-side ports of PEs. A QinQ-enabled port tags an incoming frame with its PVID.

Before you enable or disable QinQ on a port, you must remove any VLAN mappings on the port.

To enable QinQ:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>qinq enable</td>
<td>By default, QinQ is disabled.</td>
</tr>
</tbody>
</table>

Configuring transparent transmission for VLANs

You can exclude 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 the transparent VLAN.
- Do not configure any other VLAN manipulation actions for the transparent VLAN on the port.
- Make sure all ports on the traffic path permit the transparent VLAN to pass through.
- If you use both transparent VLANs and VLAN mappings on an interface, the transparent VLANs cannot be the following VLANs:
  - Original or translated VLANs of one-to-one, many-to-one, and one-to-two VLAN mappings.
  - Original or translated outer VLANs of two-to-two VLAN mappings.

To enable transparent transmission for a list of VLANs:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the port link type.</td>
<td>port link-type { hybrid</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the port to allow packets from its PVID and the transparent VLANs to pass through.</td>
<td>• For the hybrid port:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port hybrid vlan vlan-id-list { tagged</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For the trunk port:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port trunk permit vlan { vlan-id-list</td>
</tr>
<tr>
<td>5.</td>
<td>Specify transparent VLANs.</td>
<td>qinq transparent-vlan vlan-id-list</td>
</tr>
</tbody>
</table>

### Configuring the TPID for VLAN tags

TPID identifies a frame as an 802.1Q tagged frame. The TPID value varies by vendor. On an HPE 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 between directly connected devices so 802.1Q tagged frames can be identified correctly.

TPID settings include CVLAN TPID and SVLAN TPID.

A QinQ-enabled port uses the CVLAN TPID to match incoming tagged frames. An incoming frame is handled as untagged if its TPID is different from the CVLAN TPID. The device does not modify the TPID in CVLAN tags.

SVLAN TPIDs are configurable on a per-port basis. A service provider-side port uses the SVLAN TPID to replace the TPID in outgoing frames’ SVLAN tags and match incoming tagged frames. An incoming frame is handled as untagged if the TPID in its outer VLAN tag is different from the SVLAN TPID.

For example, a PE device is connected to a customer device that uses the TPID 0x8200 and to a provider device that uses the TPID 0x9100. For correct packet processing, you must set the CVLAN TPID and SVLAN TPID to 0x8200 and 0x9100 on the PE, respectively.

The TPID field is at 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 19.

### Table 19 Reserved EtherType values

<table>
<thead>
<tr>
<th>Protocol type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>0x0806</td>
</tr>
<tr>
<td>PUP</td>
<td>0x0200</td>
</tr>
<tr>
<td>RARP</td>
<td>0x8035</td>
</tr>
<tr>
<td>IP</td>
<td>0x0800</td>
</tr>
<tr>
<td>IPv6</td>
<td>0x86dd</td>
</tr>
<tr>
<td>PPPoE</td>
<td>0x8863/0x8864</td>
</tr>
<tr>
<td>MPLS</td>
<td>0x8847/0x8848</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Value</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
</tr>
<tr>
<td>IPX/SPX</td>
<td>0x8137</td>
</tr>
<tr>
<td>IS-IS</td>
<td>0x8000</td>
</tr>
<tr>
<td>LACP</td>
<td>0x8809</td>
</tr>
<tr>
<td>LLDP</td>
<td>0x88cc</td>
</tr>
<tr>
<td>802.1X</td>
<td>0x888e</td>
</tr>
<tr>
<td>802.1ag</td>
<td>0x8902</td>
</tr>
<tr>
<td>Cluster</td>
<td>0x88a7</td>
</tr>
<tr>
<td>Reserved</td>
<td>0xffff</td>
</tr>
</tbody>
</table>

Configuring the TPID for CVLAN tags

Perform this task on the PE device.

To configure the TPID value for CVLAN tags:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the TPID value for CVLAN tags.</td>
<td>qinq ethernet-type customer-tag hex-value</td>
</tr>
</tbody>
</table>

Configuring the TPID for SVLAN tags

Perform this task on the service provider-side ports of PEs.

When you configure the TPID value for SVLAN tags on a port, do not enable QinQ or EVB on it.

To configure the TPID value for SVLAN tags:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the TPID value for SVLAN tags.</td>
<td>qinq ethernet-type service-tag hex-value</td>
</tr>
</tbody>
</table>

Setting the 802.1p priority in SVLAN tags

By default, the 802.1p priority in the SVLAN tag added by a QinQ-enabled port depends on the priority trust mode on the port.

- If the 802.1p priority in frames is trusted, the device copies the 802.1p priority in the CVLAN tag to the SVLAN tag.
- If the 802.1p priority in frames is not trusted, the device copies the port priority (0 by default) to the SVLAN tag.

To set the 802.1p priority in SVLAN tags:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a traffic class and enter its view.</td>
<td>traffic classifier classifier-name [ operator ( and</td>
</tr>
<tr>
<td>3.</td>
<td>Configure CVLAN match criteria.</td>
<td>• Match CVLAN IDs: if-match customer-vlan-id vlan-id-list&lt;br&gt;• Match 802.1p priority: if-match customer-dot1p dot1p-value &amp;&lt;1-8&gt;</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Create a traffic behavior and enter its view.</td>
<td>traffic behavior behavior-name</td>
</tr>
<tr>
<td>6.</td>
<td>Configure a priority marking action for SVLAN tags.</td>
<td>• Replace the priority in the SVLAN tags of matching frames with the configured priority: remark dot1p dot1p-value&lt;br&gt;• Copy the 802.1p priority in the CVLAN tag to the SVLAN tag: remark dot1p customer-dot1p-trust</td>
</tr>
<tr>
<td>7.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>8.</td>
<td>Create a QoS policy and enter its view.</td>
<td>qos policy policy-name</td>
</tr>
<tr>
<td>9.</td>
<td>Specify the traffic behavior for the traffic class in the QoS policy.</td>
<td>classifier classifier-name behavior behavior-name</td>
</tr>
<tr>
<td>10.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>11.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>12.</td>
<td>Configure the port to trust the 802.1p priority in incoming frames.</td>
<td>qos trust dot1p</td>
</tr>
<tr>
<td>13.</td>
<td>Enable QinQ.</td>
<td>qinq enable</td>
</tr>
<tr>
<td>14.</td>
<td>Apply the QoS policy to the inbound direction of the port.</td>
<td>qos apply policy policy-name inbound</td>
</tr>
</tbody>
</table>

For more information about QoS policies, see ACL and QoS Configuration Guide.

Displaying and maintaining QinQ

Execute display commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display QinQ-enabled ports.</td>
<td>display qinq</td>
</tr>
</tbody>
</table>
QinQ configuration examples

Basic QinQ configuration example

Network requirements

As shown in Figure 78:
- The service provider assigns VLAN 100 to Company A's VLANs 10 through 70.
- The service provider assigns VLAN 200 to Company B's VLANs 30 through 90.
- The devices between PE 1 and PE 2 in the service provider network use a TPID value of 0x8200.

Configure QinQ on PE 1 and PE 2 to transmit traffic in VLANs 100 and 200 for Company A and Company B, respectively.

For the QinQ frames to be identified correctly, set the SVLAN TPID to 0x8200 on the service provider-side ports of PE 1 and PE 2.

Figure 78 Network diagram

Configuration procedure

1. Configure PE 1:
   # Configure Ten-GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 100.
   <PE1> system-view
   [PE1] interface ten-gigabitethernet 1/0/1
   [PE1-Ten-GigabitEthernet1/0/1] port link-type trunk
   [PE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
   # Set the PVID of Ten-GigabitEthernet 1/0/1 to VLAN 100.
[PE1-Ten-GigabitEthernet1/0/1] port trunk pvid vlan 100

# Enable QinQ on Ten-GigabitEthernet 1/0/1.
[PE1-Ten-GigabitEthernet1/0/1] qinq enable
[PE1-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 200.
[PE1] interface ten-gigabitethernet 1/0/2
[PE1-Ten-GigabitEthernet1/0/2] port link-type trunk
[PE1-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 200

# Set the TPID value in the SVLAN tags to 0x8200 on Ten-GigabitEthernet 1/0/2.
[PE1-Ten-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE1-Ten-GigabitEthernet1/0/2] quit

# Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 200.
[PE1] interface ten-gigabitethernet 1/0/3
[PE1-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE1-Ten-GigabitEthernet1/0/3] port trunk permit vlan 200

# Set the PVID of Ten-GigabitEthernet 1/0/3 to VLAN 200.
[PE1-Ten-GigabitEthernet1/0/3] port trunk pvid vlan 200

# Enable QinQ on Ten-GigabitEthernet 1/0/3.
[PE1-Ten-GigabitEthernet1/0/3] qinq enable
[PE1-Ten-GigabitEthernet1/0/3] quit

2. Configure PE 2:

# Configure Ten-GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 200.
<PE2> system-view

[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] port link-type trunk
[PE2-Ten-GigabitEthernet1/0/1] port trunk permit vlan 200

# Set the PVID of Ten-GigabitEthernet 1/0/1 to VLAN 200.
[PE2-Ten-GigabitEthernet1/0/1] port trunk pvid vlan 200

# Enable QinQ on Ten-GigabitEthernet 1/0/1.
[PE2-Ten-GigabitEthernet1/0/1] qinq enable
[PE2-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 200.
[PE2] interface ten-gigabitethernet 1/0/2
[PE2-Ten-GigabitEthernet1/0/2] port link-type trunk
[PE2-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 200

# Set the TPID value in the SVLAN tags to 0x8200 on Ten-GigabitEthernet 1/0/2.
[PE2-Ten-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-Ten-GigabitEthernet1/0/2] quit

# Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 100.
[PE2] interface ten-gigabitethernet 1/0/3
[PE2-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE2-Ten-GigabitEthernet1/0/3] port trunk permit vlan 100

# Set the PVID of Ten-GigabitEthernet 1/0/3 to VLAN 100.
[PE2-Ten-GigabitEthernet1/0/3] port trunk pvid vlan 100

# Enable QinQ on Ten-GigabitEthernet 1/0/3.
[PE2-Ten-GigabitEthernet1/0/3] qinq enable
[PE2-Ten-GigabitEthernet1/0/3] quit
3. Configure the devices between PE 1 and PE 2:
   # Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. (Details not shown.)
   # Configure all 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 79:

- 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 79 Network diagram

Configuration procedure

1. Configure PE 1:
   # Configure Ten-GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 100 and 3000.
   <PE1> system-view
   [PE1] interface ten-gigabitethernet 1/0/1
   [PE1-Ten-GigabitEthernet1/0/1] port link-type trunk
   [PE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 3000
   # Set the PVID of Ten-GigabitEthernet 1/0/1 to VLAN 100.
   [PE1-Ten-GigabitEthernet1/0/1] port trunk pvid vlan 100
   # Enable QinQ on Ten-GigabitEthernet 1/0/1.
   [PE1-Ten-GigabitEthernet1/0/1] qinq enable
   # Enable transparent transmission for VLAN 3000 on Ten-GigabitEthernet 1/0/1.
   [PE1-Ten-GigabitEthernet1/0/1] qinq transparent-vlan 3000
   [PE1-Ten-GigabitEthernet1/0/1] quit
   # Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 3000.
   [PE1] interface ten-gigabitethernet 1/0/2
   [PE1-Ten-GigabitEthernet1/0/2] port link-type trunk
   [PE1-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 3000
   # Set the PVID of Ten-GigabitEthernet 1/0/2 to VLAN 100.
   [PE1-Ten-GigabitEthernet1/0/2] port trunk pvid vlan 100
   # Enable QinQ on Ten-GigabitEthernet 1/0/2.
   [PE1-Ten-GigabitEthernet1/0/2] qinq enable
   # Enable transparent transmission for VLAN 3000 on Ten-GigabitEthernet 1/0/2.
   [PE1-Ten-GigabitEthernet1/0/2] qinq transparent-vlan 3000
   [PE1-Ten-GigabitEthernet1/0/2] quit

253
Configure PE 2:

# Configure Ten-GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 100 and 3000.

<PE2> system-view

[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] port link-type trunk
[PE2-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 3000

# Set the PVID of Ten-GigabitEthernet 1/0/1 to VLAN 100.

[PE1-Ten-GigabitEthernet1/0/1] port trunk pvid vlan 100

# Enable QinQ on Ten-GigabitEthernet 1/0/1.

[PE2-Ten-GigabitEthernet1/0/1] qinq enable

# Enable transparent transmission for VLAN 3000 on Ten-GigabitEthernet 1/0/1.

[PE2-Ten-GigabitEthernet1/0/1] qinq transparent-vlan 3000

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 100 and 3000.

[PE2] interface ten-gigabitethernet 1/0/2
[PE2-Ten-GigabitEthernet1/0/2] port link-type trunk
[PE2-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 3000

3. Configure the devices between PE 1 and PE 2:

# Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. (Details not shown.)

# Configure all 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 outer and inner VLAN IDs of double tagged traffic with a new pair of VLAN IDs.

VLAN mapping application scenarios

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

Figure 80 shows a typical application scenario of one-to-one and many-to-one VLAN mapping. The scenario implements broadband Internet access for a community.
As shown in Figure 80, 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.

One-to-two and two-to-two VLAN mapping

Figure 81 shows a typical application scenario of one-to-two and two-to-two VLAN mapping. In this scenario, the two remote sites of the same VPN must communicate across two SP networks.
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 82 shows a simplified network that illustrates basic VLAN mapping terms.

Basic VLAN mapping terms include the following:

- **Uplink traffic**—Traffic transmitted from the customer network to the service provider network.
- **Downlink traffic**—Traffic transmitted from the service provider network to the customer network.
- **Network-side port**—A port connected to or closer to the service provider network.
- **Customer-side port**—A port connected to or closer to the customer network.
One-to-one VLAN mapping

As shown in Figure 83, 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.

Many-to-one VLAN mapping

As shown in Figure 84, 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 or ARP snooping table. For more information about DHCP and ARP snooping, see Layer 3—IP Services Configuration Guide.
One-to-two VLAN mapping

As shown in Figure 85, one-to-two VLAN mapping is implemented on the customer-side port to add the SVLAN tag for the uplink traffic.

For the downlink traffic to be correctly sent to the customer network, make sure the SVLAN tag is removed on the customer-side port before transmission. Use one of the following methods to remove the SVLAN tag from the downlink traffic:

- Configure the customer-side port as a hybrid port and assign the port to the SVLAN as an untagged member.
- Configure the customer-side port as a trunk port and set the port PVID to the SVLAN.

Figure 85 One-to-two VLAN mapping implementation

Two-to-two VLAN mapping

As shown in Figure 86, 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.
VLAN mapping configuration task list

When you configure VLAN mapping, follow these guidelines:

- To add VLAN tags to packets, you can configure both VLAN mapping and QinQ. VLAN mapping takes effect if a configuration conflict occurs. For more information about QinQ, see "Configuring QinQ."

- To add or replace VLAN tags for packets, you can configure both VLAN mapping and a QoS policy. The QoS policy takes effect if a configuration conflict occurs. For information about QoS policies, see [ACL and QoS Configuration Guide](#).

- The following features are mutually exclusive with one another on a Layer 2 Ethernet interface or Layer 2 aggregate interface:
  - EVB.
  - VLAN mapping.
  - Binding an Ethernet service instance to a VSI or to an MPLS L2VPN cross-connect.

  Do not configure these features simultaneously on the same interface. Otherwise, the features cannot take effect.

**IMPORTANT:**
Use the appropriate VLAN mapping methods for the devices in the network.

To configure VLAN mapping:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring one-to-one VLAN mapping</td>
<td>Configure one-to-one VLAN mapping on the wiring-closet switch, as shown in Figure 80.</td>
</tr>
<tr>
<td>Configuring many-to-one VLAN mapping</td>
<td>Configure many-to-one VLAN mapping on the campus switch, as shown in Figure 80.</td>
</tr>
<tr>
<td>• Configuring many-to-one VLAN mapping in a network with dynamic IP address assignment</td>
<td></td>
</tr>
<tr>
<td>• Configuring many-to-one VLAN mapping in a network with static IP address assignment</td>
<td></td>
</tr>
<tr>
<td>Configuring one-to-two VLAN mapping</td>
<td>Configure one-to-two VLAN mapping on PE 1 and PE 4, as shown in Figure 81, through which traffic from customer networks enters the service provider networks.</td>
</tr>
<tr>
<td>Configuring two-to-two VLAN mapping</td>
<td>Configure two-to-two VLAN mapping on PE 3, as shown in Figure 81, which is an edge device of the SP 2 network.</td>
</tr>
</tbody>
</table>
Configuring one-to-one VLAN mapping

Configure one-to-one VLAN mapping on the customer-side ports of wiring-closet switches (see Figure 80) 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view. | • Enter Layer 2 Ethernet interface view: interface interface-type interface-number  
• Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number | N/A |
| 3.   | Set the link type of the port. | • Set the port link type to trunk: port link-type trunk  
• Set the port link type to hybrid: 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. | • For the trunk port: port trunk permit vlan vlan-id-list  
• For the hybrid port: port hybrid vian vlan-id-list tagged | N/A |
| 5.   | Configure a one-to-one VLAN mapping. | vlan mapping vlan-id translated-vlan vlan-id | By default, no VLAN mapping is configured on an interface. |

Configuring many-to-one VLAN mapping

Configure many-to-one VLAN mapping on campus switches (see Figure 80) to transmit the same type of traffic from different users in one VLAN.

Configuring many-to-one VLAN mapping in a network with dynamic IP address assignment

In a network that uses dynamic address assignment, configure many-to-one VLAN mapping with DHCP snooping.

The switch replaces the SVLAN tag of the downlink traffic with the associated CVLAN tag based on the DHCP snooping entry lookup.

Configuration restrictions and guidelines

When you configure many-to-one VLAN mapping in a network that uses dynamic address assignment, follow these restrictions and guidelines:

- Before you configure many-to-one VLAN mapping, create the original VLANs and the translated VLANs.
To ensure correct traffic forwarding from the service provider network to the customer network, do not configure many-to-one VLAN mapping together with uRPF. For more information about uRPF, see Security Configuration Guide.

To modify many-to-one VLAN mappings, first use the `reset dhcp snooping binding` command to clear the DHCP snooping entries.

### Many-to-one VLAN mapping configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling DHCP snooping</td>
</tr>
<tr>
<td>Enabling ARP detection</td>
</tr>
<tr>
<td>Configuring the customer-side port</td>
</tr>
<tr>
<td>Configuring the network-side port</td>
</tr>
</tbody>
</table>

### Enabling DHCP snooping

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable DHCP snooping.</td>
<td>dhcp snooping enable</td>
<td>By default, DHCP snooping is disabled. For more information about DHCP snooping configuration commands, see Layer 3—IP Services Command Reference.</td>
</tr>
</tbody>
</table>

### Enabling ARP detection

Enable ARP detection for the original VLANs and the translated VLANs.

To enable ARP detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter VLAN view.</td>
<td>vlan vlan-id</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable ARP detection.</td>
<td>arp detection enable</td>
<td>By default, ARP detection is disabled. For more information about ARP detection configuration commands, see Security Command Reference.</td>
</tr>
</tbody>
</table>

### Configuring the customer-side port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view. | • Enter Layer 2 Ethernet interface view: 
  * interface interface-type interface-number*  
  • Enter Layer 2 aggregate interface view: 
  * interface bridge-aggregation interface-number* | N/A |
| 3. Set the link type of the port. | • Set the port link type to trunk: 
  * port link-type trunk*  
  • Set the port link type to hybrid: | By default, the link type of a port is access. |
### Configuring the network-side port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Set the link type of the port.</td>
<td>By default, the link type of a port is <em>access</em>.</td>
</tr>
<tr>
<td>4.</td>
<td>Assign the port to the translated VLANs.</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the port as a DHCP snooping trusted port.</td>
<td>By default, all ports that support DHCP snooping are untrusted ports when DHCP snooping is enabled.</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the port as an ARP trusted port.</td>
<td>By default, all ports are ARP untrusted ports.</td>
</tr>
<tr>
<td>7.</td>
<td>Configure the port to use the original VLAN tags of the many-to-one mapping to replace the VLAN tags of the packets destined for the user network.</td>
<td>By default, the port does not replace the VLAN tags of the packets destined for the user network.</td>
</tr>
</tbody>
</table>
Configuring many-to-one VLAN mapping in a network with static IP address assignment

In a network that uses static IP addresses, configure many-to-one VLAN mapping with ARP snooping.

The switch replaces the SVLAN tag of the downlink traffic with the associated CVLAN tag based on the ARP snooping entry lookup.

**Configuration restrictions and guidelines**

When you configure many-to-one VLAN mapping in a network that uses static address assignment, follow these restrictions and guidelines:

- Before you configure many-to-one VLAN mapping, create the original VLANs and the translated VLANs.
- Make sure hosts in different CVLANs do not use the same IP address.
- When an IP address is no longer associated with the MAC address and VLAN in an ARP snooping entry, wait for this entry to be aged out. You can also use the `reset arp snooping ip ip-address` command to clear the entry.
- 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.
- To ensure correct traffic forwarding from the service provider network to the customer network, do not configure many-to-one VLAN mapping together with uRPF. For more information about uRPF, see Security Configuration Guide.

**Configuration task list**

**Tasks at a glance**

| Enabling ARP snooping | Configuring the customer-side port | Configuring the network-side port |

**Enabling ARP snooping**

Enable ARP snooping for the original VLANs and the translated VLANs.

To enable ARP snooping:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>vlan vlan-id</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>arp snooping enable</td>
<td>By default, ARP snooping is disabled. For more information about ARP snooping commands, see Layer 3—IP Services Command Reference.</td>
</tr>
</tbody>
</table>

**Configuring the customer-side port**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Configuring the network-side port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>Enter Layer 2 Ethernet interface view: interface interface-type interface-number Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the link type of the port.</td>
<td>Set the port link type to trunk: port link-type trunk Set the port link type to hybrid: port link-type hybrid</td>
</tr>
<tr>
<td>4.</td>
<td>Assign the port to the translated VLANs.</td>
<td>For the trunk port: port trunk permit vlan vlan-id-list For the hybrid port: port hybrid vlan vlan-id-list tagged</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the port to use the original VLAN tags of the many-to-one mapping to replace the VLAN tags of the packets destined for the user network.</td>
<td>vlan mapping nni</td>
</tr>
</tbody>
</table>

By default, the link type of a port is access.

N/A
Configuring one-to-two VLAN mapping

Configure one-to-two VLAN mapping on the customer-side ports of edge devices from which customer traffic enters SP networks, for example, on PEs 1 and 4 in Figure 81. One-to-two VLAN mapping enables the edge devices to add an SVLAN tag to each incoming packet.

Before you configure one-to-two VLAN mapping, create the CVLAN and the SVLAN.

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet in the service provider network.

To configure one-to-two VLAN mapping:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type interface-number  • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the link type of the port.</td>
<td>• Set the port link type to trunk: port link-type trunk  • Set the port link type to hybrid: port link-type hybrid</td>
</tr>
<tr>
<td>4.</td>
<td>Assign the port to the CVLANs.</td>
<td>• For the trunk port: port trunk permit vlan vlan-id-list  • For the hybrid port: port hybrid vlan vlan-id-list { tagged</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the port to allow packets from the SVLAN to pass through untagged.</td>
<td>• For the trunk port:  a. Configure the SVLAN as the PVID of the trunk port: port trunk pvid vlan vlan-id  b. Assign the trunk port to the SVLAN: port trunk permit vlan { vlan-id-list</td>
</tr>
<tr>
<td>6.</td>
<td>Configure a one-to-two VLAN mapping.</td>
<td>vlan mapping nest { range vlan-range-list</td>
</tr>
</tbody>
</table>
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 81. 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type interface-number &lt;br&gt; • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the link type of the port.</td>
<td>• Set the port link type to trunk: port link-type trunk &lt;br&gt; • Set the port link type to hybrid: port link-type hybrid</td>
</tr>
<tr>
<td>4.</td>
<td>Assign the port to the original VLANs and the translated VLANs.</td>
<td>• For the trunk port: port trunk permit vlan vlan-id-list &lt;br&gt; • For the hybrid port: port hybrid vlan vlan-id-list tagged</td>
</tr>
<tr>
<td>5.</td>
<td>Configure a two-to-two VLAN mapping.</td>
<td>vlan mapping tunnel outer-vlan-id inner-vlan-id translated-vlan outer-vlan-id inner-vlan-id</td>
</tr>
</tbody>
</table>

Displaying and maintaining VLAN mapping

Execute display commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display VLAN mapping information.</td>
<td>display vlan mapping [ interface interface-type interface-number ]</td>
</tr>
</tbody>
</table>

VLAN mapping configuration examples

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

Network requirements

As shown in Figure 87:
- Each household subscribes to PC, VoD, and VoIP services, and obtains the IP address through DHCP.
- On the home gateways, VLANs 1, 2, and 3 are assigned to PC, VoD, and VoIP traffic, respectively.

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

To save VLAN resources, configure many-to-one VLAN mappings on the campus switch (Switch C). This feature transmits the same type of traffic from different households in one VLAN. Use VLANs 501, 502, and 503 for PC, VoD, and VoIP traffic, respectively.

**Table 20 VLAN mappings for each service**

<table>
<thead>
<tr>
<th>Service</th>
<th>VLANs on home gateways</th>
<th>VLANs on wiring-closet switches (Switch A and Switch B)</th>
<th>VLANs on campus switch (Switch C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>VLAN 1</td>
<td>VLANs 101, 102, 103, 104</td>
<td>VLAN 501</td>
</tr>
<tr>
<td>VoD</td>
<td>VLAN 2</td>
<td>VLANs 201, 202, 203, 204</td>
<td>VLAN 502</td>
</tr>
<tr>
<td>VoIP</td>
<td>VLAN 3</td>
<td>VLANs 301, 302, 303, 304</td>
<td>VLAN 503</td>
</tr>
</tbody>
</table>
Figure 87 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 customer-side port Ten-GigabitEthernet 1/0/1 as a trunk port.
   <SwitchA> system-view
   [SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
# Assign Ten-GigabitEthernet 1/0/1 to all original VLANs and translated VLANs.
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301

# Configure one-to-one VLAN mappings on Ten-GigabitEthernet 1/0/1 to map VLANs 1, 2, and 3 to VLANs 101, 201, and 301, respectively.
[SwitchA-Ten-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
[SwitchA-Ten-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201
[SwitchA-Ten-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301
[SwitchA-Ten-GigabitEthernet1/0/1] quit

# Configure customer-side port Ten-GigabitEthernet 1/0/2 as a trunk port.
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/2 to all original VLANs and translated VLANs.
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302

# Configure one-to-one VLAN mappings on Ten-GigabitEthernet 1/0/2 to map VLANs 1, 2, and 3 to VLANs 102, 202, and 302, respectively.
[SwitchA-Ten-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102
[SwitchA-Ten-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202
[SwitchA-Ten-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302
[SwitchA-Ten-GigabitEthernet1/0/2] quit

# Configure the network-side port (Ten-GigabitEthernet 1/0/3) as a trunk port.
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/3 to the translated VLANs.
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
[SwitchA-Ten-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-vlan104] vlan 104
[SwitchC-vlan104] arp detection enable
[SwitchC-vlan204] vlan 204
[SwitchC-vlan204] arp detection enable
[SwitchC-vlan304] vlan 304
[SwitchC-vlan304] arp detection enable
[SwitchC-vlan501] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan502] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan503] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit

# Configure customer-side port Ten-GigabitEthernet 1/0/1 as a trunk port.
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/1 to all original VLANs and translated VLANs.
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 101 102 201 202 301 302 501 to 503

# Configure many-to-one VLAN mappings on Ten-GigabitEthernet 1/0/1 to map VLANs for PC, VoD, and VoIP traffic to VLANs 501, 502, and 503, respectively.
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping uni range 101 to 102 translated-vlan 501
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping uni range 201 to 202 translated-vlan 502
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping uni range 301 to 302 translated-vlan 503

# Enable DHCP snooping entry recording on Ten-GigabitEthernet 1/0/1.
[SwitchC-Ten-GigabitEthernet1/0/1] dhcp snooping binding record
[SwitchC-Ten-GigabitEthernet1/0/1] quit

# Configure customer-side port Ten-GigabitEthernet 1/0/2 as a trunk port.
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/2 to all original VLANs and translated VLANs.
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 103 104 203 204 303 304 501 to 503

# Configure many-to-one VLAN mappings on Ten-GigabitEthernet 1/0/2 to map VLANs for PC, VoD, and VoIP traffic to VLANs 501, 502, and 503, respectively.
[SwitchC-Ten-GigabitEthernet1/0/2] vlan mapping uni range 103 to 104 translated-vlan 501
[SwitchC-Ten-GigabitEthernet1/0/2] vlan mapping uni range 203 to 204 translated-vlan 502
[SwitchC-Ten-GigabitEthernet1/0/2] vlan mapping uni range 303 to 304 translated-vlan 503

# Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/2.
[SwitchC-Ten-GigabitEthernet1/0/2] dhcp snooping binding record
# Configure the network-side port (Ten-GigabitEthernet 1/0/3) to use the original VLAN tags of the many-to-one mappings to replace the VLAN tags of the packets destined for the user network.

```plaintext
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] vlan mapping nni
```

# Configure the network-side port Ten-GigabitEthernet 1/0/3 as a trunk port.

```plaintext
[SwitchC-Ten-GigabitEthernet1/0/3] port link-type trunk
```

# Assign Ten-GigabitEthernet 1/0/3 to the translated VLANs.

```plaintext
[SwitchC-Ten-GigabitEthernet1/0/3] port trunk permit vlan 501 to 503
```

# Configure Ten-GigabitEthernet 1/0/3 as a DHCP snooping trusted and ARP trusted port.

```plaintext
[SwitchC-Ten-GigabitEthernet1/0/3] dhcp snooping trust
[SwitchC-Ten-GigabitEthernet1/0/3] arp detection trust
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

4. Configure Switch D:

```plaintext
# Create the translated VLANs.
<SwitchD> system-view
[SwitchD] vlan 501 to 503
```

# Configure Ten-GigabitEthernet 1/0/1 as a trunk port.

```plaintext
<SwitchD> system-view
[SwitchD] interface ten-gigabitethernet 1/0/1
[SwitchD-Ten-GigabitEthernet1/0/1] port link-type trunk
```

# Assign Ten-GigabitEthernet 1/0/1 to the translated VLANs.

```plaintext
[SwitchD-Ten-GigabitEthernet1/0/1] port trunk permit vlan 501 to 503
[SwitchD-Ten-GigabitEthernet1/0/1] quit
```

### Verifying the configuration

# Verify VLAN mapping information on the wiring-closet switches, for example, Switch A.

```plaintext
[SwitchA] display vlan mapping
```

Interface Ten-GigabitEthernet1/0/1:

<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/A</td>
<td>101</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>N/A</td>
<td>201</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
<td>301</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Interface Ten-GigabitEthernet1/0/2:

<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N/A</td>
<td>102</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>N/A</td>
<td>202</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
<td>302</td>
<td>N/A</td>
</tr>
</tbody>
</table>

# Verify VLAN mapping information on Switch C.

```plaintext
[SwitchC] display vlan mapping
```

Interface Ten-GigabitEthernet1/0/1:

<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>101-102</td>
<td>N/A</td>
<td>501</td>
<td>N/A</td>
</tr>
<tr>
<td>201-202</td>
<td>N/A</td>
<td>502</td>
<td>N/A</td>
</tr>
<tr>
<td>301-302</td>
<td>N/A</td>
<td>503</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Interface Ten-GigabitEthernet1/0/2:

<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>102-102</td>
<td>N/A</td>
<td>502</td>
<td>N/A</td>
</tr>
<tr>
<td>202-202</td>
<td>N/A</td>
<td>503</td>
<td>N/A</td>
</tr>
</tbody>
</table>
One-to-two and two-to-two VLAN mapping configuration example

Network requirements

As shown in Figure 88:

- Two VPN A branches, Site 1 and Site 2, are in VLAN 5 and VLAN 6, respectively.
- The two sites use different VPN access services from different service providers, SP 1 and SP 2.
- SP 1 assigns VLAN 100 to Site 1 and Site 2. SP 2 assigns VLAN 200 to Site 1 and Site 2.

Configure one-to-two VLAN mappings and two-to-two VLAN mappings to enable the two branches to communicate across networks SP 1 and SP 2.

Figure 88 Network diagram

Configuration procedure

1. Configure PE 1:

   # Create VLANs 5 and 100.
   <PE1> system-view
   [PE1] vlan 5
   [PE1-vlan5] quit
   [PE1] vlan 100
   [PE1-vlan100] quit

   # Configure a one-to-two VLAN mapping on the customer-side port (Ten-GigabitEthernet 1/0/1) to add SVLAN tag 100 to packets from VLAN 5.
   [PE1] interface ten-gigabitethernet 1/0/1
   [PE1-Ten-GigabitEthernet1/0/1] vlan mapping nest single 5 nested-vlan 100

   # Configure Ten-GigabitEthernet 1/0/1 as a hybrid port.
   [PE1-Ten-GigabitEthernet1/0/1] port link-type hybrid

   # Assign Ten-GigabitEthernet 1/0/1 to VLAN 5 as a tagged member.
   [PE1-Ten-GigabitEthernet1/0/1] port hybrid vlan 5 tagged
2. Configure PE 2:

# Create VLAN 100.
<PE2> system-view
[PE2] vlan 100
[PE2-vlan100] quit

# Configure Ten-GigabitEthernet 1/0/1 as a trunk port.
[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/1 to VLAN 100.
[PE2-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[PE2-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port.
[PE2] interface ten-gigabitethernet 1/0/2
[PE2-Ten-GigabitEthernet1/0/2] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/2 to VLAN 100.
[PE2-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE2-Ten-GigabitEthernet1/0/2] quit

3. Configure PE 3:

# Create VLANs 5, 6, 100, and 200.
<PE3> system-view
[PE3] vlan 5 to 6
[PE3] vlan 100
[PE3-vlan100] quit
[PE3] vlan 200
[PE3-vlan200] quit

# Configure Ten-GigabitEthernet 1/0/1 as a trunk port.
[PE3] interface ten-gigabitethernet 1/0/1
[PE3-Ten-GigabitEthernet1/0/1] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/1 to VLANs 100 and 200.
[PE3-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200

# Configure a two-to-two VLAN mapping on Ten-GigabitEthernet 1/0/1 to map SVLAN 100 and CVLAN 5 to SVLAN 200 and CVLAN 6.
[PE3-Ten-GigabitEthernet1/0/1] vlan mapping tunnel 100 5 translated-vlan 200 6
[PE3-Ten-GigabitEthernet1/0/1] quit

# Configure Ten-GigabitEthernet 1/0/2 as a trunk port.
[PE3] interface ten-gigabitethernet 1/0/2
[PE3-Ten-GigabitEthernet1/0/2] port link-type trunk

# Assign Ten-GigabitEthernet 1/0/2 to VLAN 200.
4. Configure PE 4:
   
   # Create VLANs 6 and 200.
   
   <PE4> system-view
   [PE4] vlan 6
   [PE4-vlan6] quit
   [PE4] vlan 200
   [PE4-vlan200] quit
   
   # Configure the network-side port (Ten-GigabitEthernet 1/0/1) as a trunk port.
   [PE4] interface ten-gigabitethernet 1/0/1
   [PE4-Ten-GigabitEthernet1/0/1] port link-type trunk
   
   # Assign Ten-GigabitEthernet 1/0/1 to VLAN 200.
   [PE4-Ten-GigabitEthernet1/0/1] port trunk permit vlan 200
   [PE4-Ten-GigabitEthernet1/0/1] quit
   
   # Configure the customer-side port (Ten-GigabitEthernet 1/0/2) as a hybrid port.
   [PE4] interface ten-gigabitethernet 1/0/2
   [PE4-Ten-GigabitEthernet1/0/2] port link-type hybrid
   
   # Assign Ten-GigabitEthernet 1/0/2 to VLAN 6 as a tagged member.
   [PE4-Ten-GigabitEthernet1/0/2] port hybrid vlan 6 tagged
   
   # Assign Ten-GigabitEthernet 1/0/2 to VLAN 200 as an untagged member.
   [PE4-Ten-GigabitEthernet1/0/2] port hybrid vlan 200 untagged
   
   # Configure a one-to-two VLAN mapping on Ten-GigabitEthernet 1/0/2 to add SVLAN tag 200 to packets from VLAN 6.
   [PE4-Ten-GigabitEthernet1/0/2] vlan mapping nest single 6 nested-vlan 200
   [PE4-Ten-GigabitEthernet1/0/2] quit

Verifying the configuration

# Verify VLAN mapping information on PE 1.
[PE1] display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
+-------------+-------------+-------------------+-------------------+
<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>N/A</td>
<td>100</td>
<td>5</td>
</tr>
</tbody>
</table>

# Verify VLAN mapping information on PE 3.
[PE3] display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
+-------------+-------------+-------------------+-------------------+
<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>5</td>
<td>200</td>
<td>6</td>
</tr>
</tbody>
</table>

# Verify VLAN mapping information on PE 4.
[PE4] display vlan mapping
Interface Ten-GigabitEthernet1/0/2:
+-------------+-------------+-------------------+-------------------+
<table>
<thead>
<tr>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Translated Outer VLAN</th>
<th>Translated Inner VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>N/A</td>
<td>200</td>
<td>6</td>
</tr>
</tbody>
</table>
Configuring PBB

Overview

IEEE 802.1ah Provider Backbone Bridge (PBB) is a MAC-in-MAC Layer 2 VPN technology. It interconnects multiple provider bridged networks to build a large-scale end-to-end Layer 2 provider bridged network.

PBB has the following advantages over QinQ:

- Reduces the MAC address table size. In a PBB-enabled service provider network, only the edge devices maintain entries for customer MAC addresses. In a QinQ-enabled service provider network, all devices must maintain entries for customer MAC addresses.
- Supports more than 16 million service instances. QinQ supports only a maximum of 4094 outer VLANs (service instances).

For more information about QinQ, see "Configuring QinQ."

PBB network model

As shown in Figure 89, the PBB network includes backbone edge bridges and backbone core bridges.

Backbone edge bridges connect customer sites or provider bridge networks to the PBB network. They encapsulate the customer MAC in the service provider MAC. Backbone core bridges forward traffic based on the service provider MAC.

Figure 89 Typical PBB network
Terminology

PBBN
A network using PBB is a provider backbone bridge network (PBBN). A PBBN is a Layer 2 switching network where Layer 2 connections are established between different nodes.

PBN
A provider bridge network (PBN) connects a PBBN to a customer network. A customer network can connect to a PBBN directly or through a PBN.

BEB
A backbone edge bridge (BEB) is an edge device in a PBBN. A BEB encapsulates frames from a customer network by using PBB. It decapsulates PBB frames from a PBBN and forwards them to a customer network. The BEB learns customer MAC addresses.

BCB
A backbone core bridge (BCB) is a core device in a PBBN. It forwards a PBB frame according to its B-MAC and B-VLAN. A BCB only forwards frames and learns MAC addresses within the PBBN. It does not learn a large number of customer MAC addresses. This reduces network deployment costs, and the PBBN is more expandable.

CE
Customer edges (CEs) are edge devices that connect customer sites or PBNs to the BEBs of the PBBN.

B-MAC and B-VLAN
A backbone MAC address (B-MAC) is a MAC address associated with a PBB bridge. A backbone VLAN (B-VLAN) is a VLAN assigned by the service provider for transmitting customer traffic on the PBBN.

For customer frames to be transmitted across a PBBN, the ingress BEB encapsulates them in MAC-in-MAC format. In the outer frame header, the source MAC address is a B-MAC of the ingress BEB, and the destination MAC is a B-MAC of the egress BEB. All devices in the PBBN forward the PBB frames based on the destination B-MAC and B-VLAN.

Uplink port and downlink port
A port that connects a BEB to a PBBN is an uplink port, and a port that connects a BEB to a customer network is a downlink port. After frames from the customer network are encapsulated in PBB frames, they are forwarded out of the corresponding uplink ports on the BEB. After PBB frames from the PBBN are decapsulated, they are forwarded out of the corresponding downlink ports on the BEB according to the customer MAC addresses.

PBB VSI and I-SID
In a PBBN, a PBB VSI represents a service provided by the service provider, and it is uniquely identified by a backbone service instance identifier (I-SID). A VSI acts as a virtual switch with all conventional Ethernet switch functions, including source MAC address learning, MAC address aging, and flooding. For more information about VSIs, see MPLS Configuration Guide.

AC
An attachment circuit (AC) is a physical or virtual link that connects a CE to a BEB.

PBB frame format
Figure 90 shows the format of a PBB frame.
Table 21 describes key fields in the frame.

### Table 21 PBB frame fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Full name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-DA</td>
<td>Backbone destination MAC address</td>
<td>Destination B-MAC, outer destination MAC address in a PBB frame. It is the MAC address of the BEB at the destination end of the PBBN tunnel. The combination of B-DA and B-SA is B-MAC.</td>
</tr>
<tr>
<td>B-SA</td>
<td>Backbone source MAC address</td>
<td>Source B-MAC, outer source MAC address in a PBB frame. It is the MAC address of the BEB at the source end of the PBBN tunnel. The combination of B-DA and B-SA is B-MAC.</td>
</tr>
<tr>
<td>B-Tag</td>
<td>Backbone VLAN tag</td>
<td>B-VLAN tag, outer VLAN tag in a PBB frame. It indicates the VLAN information and priority information of the frame within the PBBN. The TPID in a B-Tag is 0x8100.</td>
</tr>
<tr>
<td>I-Tag</td>
<td>Backbone service instance tag</td>
<td>Service identifier of a PBB frame. The I-Tag contains the following fields:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TPID—The TPID in an I-Tag is 0x88E7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I-PCP—Backbone service instance priority code point.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I-DEI—Backbone service instance drop eligibility indicator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I-SID—Backbone service instance identifier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C-DA—Destination MAC address of the customer frame.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C-SA—Source MAC address of the customer frame.</td>
</tr>
<tr>
<td>S-Tag</td>
<td>Service provider VLAN tag</td>
<td>Outer VLAN tag of the frame in the PBN, which indicates the VLAN and priority information of the frame within the PBN.</td>
</tr>
<tr>
<td>C-Tag</td>
<td>Customer VLAN tag</td>
<td>Inner VLAN tag of the frame in the PBN, which indicates the VLAN and priority information of the frame within the customer network.</td>
</tr>
</tbody>
</table>

For more information about TPID, see "Configuring VLANs."
On a PBBN, the BEBs encapsulate customer traffic in PBB, and learn their C-MAC reachability information in the data plane. To forward traffic across the PBBN, the BEBs learn unicast forwarding entries for reaching each other. Each entry contains a B-MAC address, B-VLAN, I-SID, and outgoing interface.

The following describes how a unicast forwarding entry is created:

1. When BEB 1 receives a frame with an unknown destination C-MAC (for example, MAC A) from the customer network, BEB 1 performs the following operations:
   a. Assign the frame to a PBB VSI based on the configured match criteria.
   b. Encapsulates the frame in MAC-in-MAC format. The source B-MAC is the MAC address of BEB 1. The destination B-MAC is the multicast B-MAC configured for the matching PBB VSI.
   c. Multicasts the PBB frame out of the VSI's all uplink ports.
2. When BEB 2 receives the PBB frame, it performs the following operations:
   a. Creates a unicast forwarding entry for MAC A. In the entry, the destination B-MAC is the B-MAC of BEB 1, the outgoing interface is the interface on which the frame was received.
   b. Removes the PBB encapsulation, and then forwards the frame to the customer network.

Figure 91 shows how the PBBN forwards a frame between BEBs if a unicast forwarding entry exists for the frame:

3. BEB 1 encapsulates a customer frame with the matching source and destination B-MACs, B-VLAN, and I-SID. Then it forwards the frame to the BCB through its uplink port.
4. BCB forwards the PBB frame from BEB 1 to BEB 2 according to the frame's destination B-MAC and B-VLAN.
5. BEB 2 removes the PBB encapsulation, and then forwards the original Ethernet frame out of the downlink port to the customer network.

Protocols and standards

IEEE 802.1ah, *Virtual Bridged Local Area Networks Amendment 7: Provider Backbone Bridges*
Configuration restrictions and guidelines

When you configure PBB, follow these restrictions and guidelines:

- You need to configure PBB only on BEBs.
- On BCBs, you must create VLANs that are the same as the B-VLANs used on the BEBs.

PBB configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling L2VPN</td>
</tr>
<tr>
<td>(Required.) Creating a PBB VSI</td>
</tr>
<tr>
<td>(Required.) Configuring a B-VLAN for a PBB VSI</td>
</tr>
<tr>
<td>(Required.) Configuring an uplink port</td>
</tr>
<tr>
<td>(Required.) Configuring a downlink port</td>
</tr>
<tr>
<td>(Optional.) Configuring the data encapsulation type</td>
</tr>
</tbody>
</table>

Enabling L2VPN

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable L2VPN.</td>
<td>l2vpn enable</td>
</tr>
</tbody>
</table>

Creating a PBB VSI

When you create a PBB VSI, follow these guidelines:

- You can configure one PBB I-SID and one SPB I-SID for a VSI, but the two I-SIDs must be different. For more information about SPB, see SPB Configuration Guide.
- You must assign a unique I-SID to each PBB VSI.
- The name of a PBB VSI can be different on different PBB nodes, but its I-SID must be the same across the PBBN.

To create a PBB VSI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VSI and enter VSI view.</td>
<td>vsi vsi-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the VSI as a PBB VSI, specify a PBB I-SID for the PBB VSI, and enter PBB VSI view.</td>
<td>pbb i-sid i-sid</td>
</tr>
</tbody>
</table>
Configuring a B-VLAN for a PBB VSI

You can assign only one B-VLAN to a PBB VSI, but different PBB VSIs can use the same B-VLAN. For a PBB VSI, you must specify the same I-SID and B-VLAN across all BEBs.

To configure a B-VLAN for a PBB VSI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VSI view.</td>
<td>vsi vsi-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the VSI as a PBB VSI, specify a PBB I-SID for the PBB VSI, and enter PBB VSI view.</td>
<td>pbb i-sid i-sid</td>
</tr>
<tr>
<td>4.</td>
<td>Specify a B-VLAN for the PBB VSI.</td>
<td>bvlan vlan-id</td>
</tr>
</tbody>
</table>

Configuring an uplink port

On the BEB, you must specify uplink ports for a PBB VSI to forward frames from the customer network to the service provider network.

You can specify multiple uplink ports for one PBB VSI. The device automatically selects uplink ports for packets. The uplink ports cannot be member ports in a link aggregation group.

For the uplink port configuration to take effect, perform the following tasks before uplink port assignment:

- Assign a B-VLAN to the PBB VSI.
- Verify that the port is in up state and is not a link aggregation group member.
- Assign the port to the B-VLAN.

To configure an uplink port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the port as the uplink port for the specified or all PBB VSIs.</td>
<td>pbb uplink { all</td>
</tr>
</tbody>
</table>

Configuring a downlink port

You can specify one or multiple downlink ports for a PBB VSI.

Do not assign a downlink port to a B-VLAN.

You can create Ethernet service instances on both a Layer 2 aggregate interface and its member ports and map the Ethernet service instances to VSIs. However, the Ethernet service instances on the aggregation member ports are down. For the Ethernet service instances to come up, you must remove the aggregation member ports from the aggregation group.
To configure a downlink port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Create an Ethernet service instance and enter Ethernet service instance view.</td>
<td>service-instance instance-id</td>
</tr>
</tbody>
</table>
| 4.   | Configure a match criterion. | • encapsulation s-vid vlan-id [ c-vid { vlan-id-list | all } | only-tagged ]
• encapsulation s-vid vlan-id-list [ c-vid vlan-id-list ]
• encapsulation { default | tagged | untagged } | By default, no match criterion is configured. |
| 5.   | Map the Ethernet service instance to a PBB VSI. | xconnect vsi vsi-name [ access-mode { ethernet | vlan } ] | By default, an Ethernet service instance is not mapped to any PBB VSI. |

For more information about the `service-instance`, `encapsulation`, and `xconnect vsi` commands, see *MPLS Command Reference*.

## Configuring the data encapsulation type

A PBB VSI supports Ethernet and VLAN data encapsulation types.

Data encapsulation type decides how the BEB handles the P-tag on a PBB VSI, as shown in Table 22. P-tags are unique VLAN tags that the service provider assigns to users for differentiation.

### Table 22 P-tag manipulation

<table>
<thead>
<tr>
<th>Traffic direction</th>
<th>Ethernet encapsulation</th>
<th>VLAN encapsulation</th>
</tr>
</thead>
</table>
| CE to PBBN        | The traffic must not contain a P-tag.  
• **VLAN access mode**—The BEB removes the P-tag before it encapsulates the traffic in PBB.  
• **Ethernet access mode**—The BEB directly encapsulates the traffic in PBB. The VLAN tag in the received traffic is considered a U-tag. |  
• **VLAN access mode**—The traffic must contain a P-tag.  
• **Ethernet access mode**—The BEB forwards the traffic with the P-tag modified or intact. |
| PBBN to CE        |  
• **VLAN access mode**—The BEB adds a P-tag before it forwards the traffic.  
• **Ethernet access mode**—The BEB forwards the traffic without adding a P-tag. The BEB cannot modify or remove any tags already in the traffic from PBBN to CE. |  
• **VLAN access mode**—The BEB removes the P-tag before it forwards the traffic. |

282
NOTE:
To configure the access mode, use the `xconnect vsi` command (see *MPLS Command Reference*).

To configure the data encapsulation type for a PBB VSI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter VSI view.</td>
<td><code>vsi vsi-name</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enter PBB VSI view.</td>
<td><code>pbb i-sid i-sid</code></td>
</tr>
<tr>
<td>4.</td>
<td>Specify an encapsulation</td>
<td>`encapsulation { ethernet</td>
</tr>
<tr>
<td></td>
<td>type for the PBB VSI.</td>
<td>vlan }</td>
</tr>
</tbody>
</table>

### Displaying and maintaining PBB

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display PBB VSI connections.</td>
<td><code>display pbb connection</code></td>
</tr>
<tr>
<td>Display MAC-in-MAC connections.</td>
<td><code>display l2vpn minm connection [ vsi vsi-name ]</code></td>
</tr>
<tr>
<td>Display MAC-in-MAC forwarding entries.</td>
<td><code>display l2vpn minm forwarding [ vsi vsi-name ] [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display VSI information.</td>
<td><code>display l2vpn vsi [ name vsi-name ] [ verbose ]</code></td>
</tr>
<tr>
<td>Clear PBB VSI connections.</td>
<td>`reset pbb connection [ bvlan vlan-id</td>
</tr>
</tbody>
</table>

### PBB configuration example

#### Network requirements

As shown in *Figure 92*, configure PBB to provide connectivity between network A and network B of a customer.

*Figure 92 Network diagram*
Configuration procedure

1. Configure BEB 1:
   # Create VLAN 20.
   <BEB1> system-view
   [BEB1] vlan 20
   [BEB1-vlan20] quit
   # Enable L2VPN.
   [BEB1] l2vpn enable
   # Create a VSI of the PBB type.
   [BEB1] vsi aaa
   # Specify the I-SID as 1.
   [BEB1-vsi-aaa] pbb i-sid 1
   # Specify B-VLAN 20 for the PBB VSI.
   [BEB1-vsi-aaa-1] bvlan 20
   [BEB1-vsi-aaa-1] quit
   [BEB1-vsi-aaa] quit
   # Configure Ten-GigabitEthernet 1/0/1 as a trunk port, assign it to VLAN 20, and configure it as an uplink port of the PBB VSI.
   [BEB1] interface ten-gigabitethernet 1/0/1
   [BEB1-Ten-GigabitEthernet1/0/1] port link-type trunk
   [BEB1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 20
   [BEB1-Ten-GigabitEthernet1/0/1] pbb uplink vsi aaa
   [BEB1-Ten-GigabitEthernet1/0/1] quit
   # Create Ethernet service instance 1 on Ten-GigabitEthernet 1/0/2.
   [BEB1] interface ten-gigabitethernet 1/0/2
   [BEB1-Ten-GigabitEthernet1/0/2] service-instance 1
   # Configure the Ethernet service instance to match all 802.1Q tagged frames. Map the service instance to the PBB VSI, and set the access mode to Ethernet.
   [BEB1-Ten-GigabitEthernet1/0/2-srv1] encapsulation tagged
   [BEB1-Ten-GigabitEthernet1/0/2-srv1] xconnect vsi aaa access-mode ethernet
   [BEB1-Ten-GigabitEthernet1/0/2-srv1] quit
   [BEB1-Ten-GigabitEthernet1/0/2] quit
   # Configure Ethernet encapsulation for the PBB VSI.
   [BEB1] vsi aaa
   [BEB1-vsi-aaa] pbb i-sid 1
   [BEB1-vsi-aaa-1] encapsulation ethernet
   [BEB1-vsi-aaa-1] quit

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

Verifying the configuration

# Display PBB VSI connections on BEB 1.
[BEB1] display pbb connection
BMAC     BVLAN  Port       Type  Aging
011e-8300-0001  20     XGE1/0/1   MC    N
000f-e200-0001  20     XGE1/0/1   UC    Y
# Verify that Device A and Device B can ping each other. (Details not shown.)

## Troubleshooting PBB

### Failed to transmit customer frames to peer

**Symptom**

Customer frames cannot be transmitted to the peer network by using PBB.

**Solution**

To resolve the problem:

1. Use the `display l2vpn vsi verbose` command to display the PBB configuration of the VSI.
   - If the VSI is not configured as a PBB VSI, configure the VSI as a PBB VSI.
   - If the VSI is down, use the `undo shutdown` command to bring the VSI up.

2. Use the `display l2vpn vsi verbose` command to verify that the VSI's PBB settings are consistent across BEBs, especially the I-SID and B-VLAN settings.

3. Use the `display vlan all` command to verify that the following settings are configured on all BCBs:
   - The B-VLAN is created on each BCB.
   - All ports on the path between the BEBs are assigned to the B-VLAN.

4. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring LLDP

Overview

In a heterogeneous network, a standard configuration exchange platform ensures that 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, port ID, and so on. 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. It supports a subset of the features of a MAC bridge. A TPMR is transparent to all frame-based media-independent protocols except for the following protocols:

- Protocols destined to it.
- Protocols destined to reserved MAC addresses that the relay feature of the TPMR is configured not to forward.

LLDP exchanges packets between neighbor agents and creates and maintains neighbor information for them. Figure 93 shows the neighbor relationships for these LLDP agents. LLDP has two bridge modes: customer bridge (CB) and service bridge (SB).

Figure 93 LLDP neighbor relationships
LLDP frame formats

LLDP sends device information in LLDP frames. LLDP frames are encapsulated in Ethernet II or Subnetwork Access Protocol (SNAP) frames.

- LLDP frame encapsulated in Ethernet II

**Figure 94 Ethernet II-encapsulated LLDP frame**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination MAC address | MAC address to which the LLDP frame is advertised. LLDP specifies different multicast MAC addresses as destination MAC addresses for LLDP frames destined for agents of different types. This helps distinguish between LLDP frames sent and received by different agent types on the same interface. The destination MAC address is fixed to one of the following multicast MAC addresses:  
  - 0x0180-c200-000E for LLDP frames destined for nearest bridge agents.  
  - 0x0180-c200-0000 for LLDP frames destined for nearest customer bridge agents.  
  - 0x0180-c200-0003 for LLDP frames destined for nearest non-TPMR bridge agents. |
| Source MAC address | MAC address of the sending port.                                             |
| Type          | Ethernet type for the upper-layer protocol. This field is 0x88CC for LLDP.   |
| Data          | 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 95 SNAP-encapsulated LLDP frame

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination MAC address</td>
<td>MAC address to which the LLDP frame is advertised. It is the same as that for Ethernet II-encapsulated LLDP frames.</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>MAC address of the sending port.</td>
</tr>
<tr>
<td>Type</td>
<td>SNAP type for the upper-layer protocol. This field is 0xAAAA-0300-0000-88CC for LLDP.</td>
</tr>
<tr>
<td>Data</td>
<td>LLDPDU.</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.</td>
</tr>
</tbody>
</table>

Table 24 Fields in a SNAP-encapsulated LLDP 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 96.

Figure 96 LLDPDU encapsulation format

<table>
<thead>
<tr>
<th>Chassis ID TLV</th>
<th>Port ID TLV</th>
<th>Time To Live TLV</th>
<th>Optional TLV</th>
<th>...</th>
<th>Optional TLV</th>
<th>End of LLDPDU TLV</th>
</tr>
</thead>
</table>

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 25 lists the basic management TLV types. Some of them are mandatory for LLDPDUs.
Table 25 Basic management TLVs

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID</td>
<td>Specifies the bridge MAC address of the sending device.</td>
<td></td>
</tr>
</tbody>
</table>
| Port ID            | Specifies the ID of the sending port:  
- If the LLDPDU carries LLDP-MED TLVs, the port ID TLV carries the MAC address of the sending port.  
- Otherwise, the port ID TLV carries the port name. | Mandatory. |
| 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.      |         |
| System Name        | Specifies the assigned name of the sending device.   |         |
| System Description | Specifies the description for the sending device.    |         |
| System Capabilities| Identifies the primary features of the sending device and the enabled primary features. |         |
| Management Address | Specifies the following elements:  
- The management address of the local device.  
- The interface number and object identifier (OID) associated with the address. |         |

- IEEE 802.1 organizationally specific TLVs

Table 26 IEEE 802.1 organizationally specific TLVs

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port VLAN ID (PVID)</td>
<td>Specifies the port VLAN identifier.</td>
</tr>
<tr>
<td>Port And Protocol VLAN ID (PPVID)</td>
<td>Indicates whether the device supports protocol VLANs and, if so, what VLAN IDs these protocols will be associated with.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Specifies the textual name of any VLAN to which the port belongs.</td>
</tr>
<tr>
<td>Protocol Identity</td>
<td>Indicates protocols supported on the port.</td>
</tr>
<tr>
<td>DCBX</td>
<td>Data center bridging exchange protocol.</td>
</tr>
<tr>
<td>EVB module</td>
<td>Edge Virtual Bridging module, including EVB TLV and CDCP TLV.</td>
</tr>
<tr>
<td>Link Aggregation</td>
<td>Indicates whether the port supports link aggregation, and if yes, whether link aggregation is enabled.</td>
</tr>
<tr>
<td>Management VID</td>
<td>Management VLAN ID.</td>
</tr>
<tr>
<td>VID Usage Digest</td>
<td>VLAN ID usage digest.</td>
</tr>
<tr>
<td>ETS Configuration</td>
<td>Enhanced Transmission Selection configuration.</td>
</tr>
<tr>
<td>ETS Recommendation</td>
<td>ETS recommendation.</td>
</tr>
<tr>
<td>PFC</td>
<td>Priority-based Flow Control.</td>
</tr>
<tr>
<td>APP</td>
<td>Application protocol.</td>
</tr>
<tr>
<td>QCN</td>
<td>Quantized Congestion Notification.</td>
</tr>
</tbody>
</table>
NOTE:
- HPE devices support only receiving protocol identity TLVs and VID usage digest TLVs.
- Layer 3 Ethernet ports support only link aggregation TLVs.

- IEEE 802.3 organizationally specific TLVs

  **Table 27 IEEE 802.3 organizationally specific TLVs**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC/PHY Configuration/Status</td>
<td>Contains the bit-rate and duplex capabilities of the port, support for autonegotiation, enabling status of autonegotiation, and the current rate and duplex mode.</td>
</tr>
</tbody>
</table>
| Power Via MDI               | Contains the power supply capabilities of the port:  
  - Port class (PSE or PD).  
  - Power supply mode.  
  - Whether PSE power supply is supported.  
  - Whether PSE power supply is enabled.  
  - Whether pair selection can be controlled.  
  - Power supply type.  
  - Power source.  
  - Power priority.  
  - PD requested power.  
  - PSE allocated power. |
| Maximum Frame Size          | Indicates the maximum supported frame size. This TLV displays the MTU of the port.                                                        |
| Power Stateful Control      | Indicates the power state control configured on the sending port, including the following:  
  - Power supply mode of the PSE/PD.  
  - PSE/PD priority.  
  - PSE/PD power. |
| Energy-Efficient Ethernet   | Indicates Energy Efficient Ethernet (EEE).                                                                                               |

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 28**.

  **Table 28 LLDP-MED TLVs**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP-MED Capabilities</td>
<td>Allows a network device to advertise the LLDP-MED TLVs that it supports.</td>
</tr>
<tr>
<td>Network Policy</td>
<td>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.</td>
</tr>
<tr>
<td>Extended Power-via-MDI</td>
<td>Allows a network device or terminal device to advertise power supply capability. This TLV is an extension of the Power Via MDI.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLV</td>
<td>Type of TLV.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>Allows a terminal device to advertise its hardware version.</td>
</tr>
<tr>
<td>Firmware Revision</td>
<td>Allows a terminal device to advertise its firmware version.</td>
</tr>
<tr>
<td>Software Revision</td>
<td>Allows a terminal device to advertise its software version.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Allows a terminal device to advertise its serial number.</td>
</tr>
<tr>
<td>Manufacturer Name</td>
<td>Allows a terminal device to advertise its vendor name.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Allows a terminal device to advertise its model name.</td>
</tr>
<tr>
<td>Asset ID</td>
<td>Allows a terminal device to advertise its asset ID. The typical case is</td>
</tr>
<tr>
<td></td>
<td>that the user specifies the asset ID for the endpoint to facilitate</td>
</tr>
<tr>
<td></td>
<td>directory management and asset tracking.</td>
</tr>
<tr>
<td>Location Identification</td>
<td>Allows a network device to advertise the appropriate location identifier</td>
</tr>
<tr>
<td></td>
<td>information for a terminal device to use in the context of location-based</td>
</tr>
<tr>
<td></td>
<td>applications.</td>
</tr>
</tbody>
</table>

**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 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.

The fast LLDP frame transmission mechanism successively sends the specified number of LLDP frames at a configurable fast LLDP frame transmission interval. The mechanism helps 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. The initial value of the aging timer is equal to the TTL value in the Time To Live TLV carried in the LLDP frame. When the LLDP agent receives a new LLDP frame, the aging timer restarts. When the aging timer decreases to zero, all saved information ages out.

**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**

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing basic LLDP configurations:</td>
</tr>
<tr>
<td>• (Required.) Enabling LLDP</td>
</tr>
<tr>
<td>• (Optional.) Setting the LLDP bridge mode</td>
</tr>
<tr>
<td>• (Optional.) Setting the LLDP operating mode</td>
</tr>
<tr>
<td>• (Optional.) Setting the LLDP reinitialization delay</td>
</tr>
<tr>
<td>• (Optional.) Enabling LLDP polling</td>
</tr>
<tr>
<td>• (Optional.) Configuring the advertisable TLVs</td>
</tr>
<tr>
<td>• (Optional.) Configuring the management address and its encoding format</td>
</tr>
<tr>
<td>• (Optional.) Setting other LLDP parameters</td>
</tr>
<tr>
<td>• (Optional.) Setting an encapsulation format for LLDP frames</td>
</tr>
<tr>
<td>• (Optional.) Disabling LLDP PVID inconsistency check</td>
</tr>
<tr>
<td>(Optional.) Configuring CDP compatibility</td>
</tr>
<tr>
<td>(Optional.) Configuring LLDP neighbor validation and aging</td>
</tr>
<tr>
<td>(Optional.) Configuring DCBX</td>
</tr>
<tr>
<td>(Optional.) Configuring LLDP trapping and LLDP-MED trapping</td>
</tr>
<tr>
<td>(Optional.) Setting the source MAC address of LLDP frames to the MAC address of a Layer 3 Ethernet subinterface</td>
</tr>
<tr>
<td>(Optional.) Enabling the device to generate ARP or ND entries for received management address LLDP TLVs</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>lldp global enable</td>
<td>By default: • If the device is started with the software default settings, LLDP is disabled globally. • If the device is started with the factory default settings, LLDP is enabled globally. For more information about device startup with software or factory default settings, see <em>Fundamentals Configuration Guide</em>.</td>
</tr>
<tr>
<td>3.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>lldp enable</td>
<td>By default, LLDP is enabled on a port.</td>
</tr>
</tbody>
</table>

**NOTE:**
An LLDP-enabled IRF physical interface supports only the nearest bridge agents.

Setting the LLDP bridge mode

The following LLDP bridge modes are available:

- **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.
- **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.

To set the LLDP bridge mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Setting the LLDP operating mode

1. Enter system view.
   - system-view

2. Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, Layer 2/Layer 3 aggregate interface view, or IRF physical interface view.
   - interface interface-type interface-number

3. Set the LLDP operating mode.
   - In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:
     - lldp [ agent { nearest-customer | nearest-nontpmr } ]
       - admin-status { disable | rx | tx | txrx }
   - In Layer 2/Layer 3 aggregate interface view:
     - lldp agent { nearest-customer | nearest-nontpmr }
       - admin-status { disable | rx | tx | txrx }
   - In IRF physical interface view:
     - lldp admin-status { disable | rx | tx | txrx }

By default:
- The nearest bridge agent operates in txrx mode.
- The nearest customer bridge agent and nearest non-TPMR bridge agent operate in disable mode.

In Ethernet interface view, if you do not specify an agent type, the command sets the operating mode for nearest bridge agents.
In aggregate interface view, you can set the operating mode only for nearest customer bridge agents and nearest non-TPMR bridge agents.
In IRF physical interface view, you can set the operating mode only for nearest bridge agents.

Setting the LLDP reinitialization delay

When the LLDP operating mode changes on a port, the port initializes the protocol state machines after an LLDP reinitialization delay. By adjusting the delay, you can avoid frequent initializations caused by frequent changes to the LLDP operating mode on a port.

To set the LLDP reinitialization delay for ports:

1. Enter system view.
   - system-view

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, Layer 2/Layer 3 aggregate interface view, or IRF physical interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable LLDP polling and set the polling interval.</td>
<td>• In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view: lldp [ agent { nearest-customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In Layer 2/Layer 3 aggregate interface view: lldp agent { nearest-customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In IRF physical interface view: lldp check-change-interval interval</td>
</tr>
</tbody>
</table>

Configuring the advertisable TLVs

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, Layer 2/Layer 3 aggregate interface view, or IRF physical interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the advertisable TLVs (in Layer 2 Ethernet interface view).</td>
<td>• lldp tlv-enable { basic-tlv { all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Nearest bridge agents can advertise all LLDP TLVs except the DCBX, location identification, port and protocol VLAN ID, VLAN name, and management VLAN ID, TLVs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Nearest non-TPMR bridge agents can advertise only the EVB TLV.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>**inventory</td>
<td>network-policy</td>
</tr>
<tr>
<td></td>
<td>[vlan-id]</td>
<td>power-over-ethernet</td>
</tr>
<tr>
<td></td>
<td>location-id { civic-address</td>
<td>device-type country-code</td>
</tr>
<tr>
<td></td>
<td>[ca-type ca-value ]&amp;&lt;1-10&gt;</td>
<td>elin-address tel-number } }</td>
</tr>
<tr>
<td></td>
<td>• lldp agent nearest-nontpmr</td>
<td>tlv-enable { basic-tlv { all</td>
</tr>
<tr>
<td></td>
<td>• lldp agent nearest-customer</td>
<td>tlv-enable { basic-tlv { all</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the advertisable TLVs (in Layer 3 Ethernet interface view).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• lldp tlv-enable { basic-tlv { all</td>
<td>port-description</td>
</tr>
<tr>
<td></td>
<td>• lldp agent { nearest-nontpmr</td>
<td>nearest-customer } tlv-enable { basic-tlv { all</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the advertisable TLVs (in management Ethernet interface view).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• lldp tlv-enable { basic-tlv { all</td>
<td>port-description</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Nearest bridge agents can advertise all types of LLDP TLVs (only link aggregation TLV is supported in 802.1 organizationally specific TLVs) except network policy TLVs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Nearest non-TPMR bridge agents do not advertise TLVs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the advertisable TLVs (in Layer 2 aggregate interface view).</td>
<td>- By default: Nearest non-TPMR bridge agents can advertise only EVB TLVs. Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only port and protocol VLAN ID, VLAN name, and management VLAN ID TLVs are supported). Nearest bridge agents are not supported on Layer 2 aggregate interfaces.</td>
</tr>
<tr>
<td>7.</td>
<td>Configure the advertisable TLVs (in Layer 3 aggregate interface view).</td>
<td>- By default: Nearest non-TPMR bridge agents do not advertise TLVs. Nearest customer bridge agents can advertise only basic TLVs. Nearest bridge agents are not supported on Layer 3 aggregate interfaces.</td>
</tr>
<tr>
<td>8.</td>
<td>Configure the advertisable TLVs (in IRF physical interface view).</td>
<td>- An LLDP-enabled IRF physical interface supports only the nearest bridge agent. By default, nearest bridge</td>
</tr>
</tbody>
</table>
Configuring the management address and its encoding format

LLDP encodes management addresses in numeric or string format in management address TLVs.

If a neighbor encodes its management address in string format, set the encoding format of the management address to **string** on the connecting port. This guarantees normal communication with the neighbor.

You can configure advertisement of the management address TLV globally or on a per-interface basis. The device selects the management address TLV advertisement setting for an interface in the following order:

1. Interface-based setting, configured by using the `lldp tlv-enable` command with the `management-address-tlv` keyword.
2. Global setting, configured by using the `lldp global tlv-enable basic-tlv management-address-tlv` command.
3. Default setting for the interface.

   By default:
   - The nearest bridge agent and nearest customer bridge agent advertise the management address TLV.
   - The nearest non-TPMR bridge agent does not advertise the management address TLV.

To configure advertisement of the management address TLV and set the management address encoding format:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enable advertisement of the management address TLV globally and set the management address to be advertised.</td>
<td>`lldp [ agent { nearest-customer</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
</tbody>
</table>
| 4. | Enable advertisement of the management address TLV on the interface and set the management address to be advertised. | By default:
- The nearest bridge agent and nearest customer bridge agent advertises the management address TLV.
- The nearest non-TPMR bridge agent does not advertise the management address TLV. |

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enable advertisement of the management address TLV globally and set the management address to be advertised.</td>
<td>`lldp [ agent { nearest-customer</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
</tbody>
</table>
| 4. | Enable advertisement of the management address TLV on the interface and set the management address to be advertised. | By default:
- The nearest bridge agent and nearest customer bridge agent advertises the management address TLV.
- The nearest non-TPMR bridge agent does not advertise the management address TLV. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>lldp hold-multiplier value</td>
<td>The default setting is 4.</td>
</tr>
<tr>
<td>3.</td>
<td>lldp timer tx-interval interval</td>
<td>The default setting is 30 seconds.</td>
</tr>
<tr>
<td>4.</td>
<td>lldp max-credit credit-value</td>
<td>The default setting is 5.</td>
</tr>
<tr>
<td>5.</td>
<td>lldp fast-count count</td>
<td>The default setting is 4.</td>
</tr>
<tr>
<td>6.</td>
<td>lldp timer fast-interval interval</td>
<td>The default setting is 1 second.</td>
</tr>
</tbody>
</table>

### 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. The TTL is expressed by using the following formula:

\[
\text{TTL} = \min (65535, (\text{TTL multiplier} \times \text{LLDP frame transmission interval} + 1))
\]

As the expression shows, the TTL can be up to 65535 seconds. TTLs greater than 65535 will be rounded down to 65535 seconds.

To set LLDP parameters:
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.

Earlier versions of LLDP require the same encapsulation format on both ends to process LLDP frames. To successfully communicate with a neighboring device running an earlier version of LLDP, the local device must be set with the same encapsulation format.

To set the encapsulation format for LLDP frames to SNAP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, Layer 2/Layer 3 aggregate interface view, or IRF physical interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the encapsulation format for LLDP frames to SNAP.</td>
<td>By default, Ethernet II encapsulation format applies.</td>
</tr>
</tbody>
</table>

Disabling LLDP PVID inconsistency check

By default, when the system receives an LLDP packet, it compares the PVID value contained in packet with the PVID configured on the receiving interface. If the two PVIDs do not match, a log message will be printed to notify the user.

You can disable PVID inconsistency check if different PVIDs are required on a link.

To disable LLDP PVID inconsistency check:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable LLDP PVID inconsistency check.</td>
<td>lldp ignore-pvid-inconsistency</td>
</tr>
</tbody>
</table>

By default, LLDP PVID inconsistency check is enabled.
Configuring CDP compatibility

To enable your device to exchange information with a directly connected Cisco device that supports only CDP, you must enable CDP compatibility.

CDP compatibility enables your device to receive and recognize CDP packets from the neighboring CDP device and send CDP packets to the neighboring device. The CDP packets sent to the neighboring CDP device carry the following information:

- Device ID.
- ID of the port connecting to the neighboring device.
- Port IP address.
- TTL.

The port IP address is the primary IP address of a 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 are assigned an IP address or all VLAN interfaces are down, no port IP address will be advertised.

You can view the neighboring CDP device information that can be recognized by the device in the output of the `display lldp neighbor-information` command. For more information about the `display lldp neighbor-information` command, see Layer 2—LAN Switching Command Reference.

To make your device work with Cisco IP phones, you must enable CDP compatibility.

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 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 configured voice VLAN. If no voice VLAN is configured for CDP packets, CDP packets carry the voice VLAN of the port or the voice VLAN assigned by the RADIUS server. The assigned voice VLAN has a higher priority. 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 CDP device.
- 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 a port, follow these steps:

1. Enable CDP-compatible LLDP globally.
2. Configure CDP-compatible LLDP to operate in TxRx mode on the port.

The maximum TTL value that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with CDP devices, configure the LLDP frame transmission interval to be no more than 1/3 of the TTL value.

To configure LLDP to be compatible with CDP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable CDP compatibility globally.</td>
<td>lldp compliance cdp</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, or Layer 2/Layer 3 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Configure CDP-compatible LLDP to operate in TxRx mode.</td>
<td>lldp compliance admin-status cdp txrx</td>
</tr>
<tr>
<td>5.</td>
<td>Set the voice VLAN ID carried in CDP packets.</td>
<td>cdp voice-vlan vlan-id</td>
</tr>
</tbody>
</table>

**Configuring LLDP neighbor validation and aging**

**Configuring LLDP neighbor validation on an interface**

LLDP neighbor validation enables an interface to validate the identity of the neighbor based on the neighbor validation criteria configured on the interface. The neighbor validation criteria can be the chassis ID TLV, port ID TLV, or both. Each incoming LLDP packet must match all the validation criteria configured on the interface. If the neighbor information in an incoming LLDP packet does not match the criteria, the system shuts down the data link layer and disables data transmission for the interface.

To configure LLDP neighbor validation on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 or Layer 3 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.   | Configure the neighbor validation criteria. | • Configure the chassis ID TLV criterion: lldp neighbor-identity chassis-id chassis-id-subtype chassis-id  
  • Configure the port ID TLV criterion: lldp neighbor-identity port-id port-id-subtype port-id | A minimum of one neighbor validation criterion is required on the interface for neighbor validation to work. By default, no neighbor validation criteria exist on an interface. |
Configuring LLDP neighbor aging on an interface

An LLDP neighbor aging-enabled interface ages out a neighbor if it does not receive an LLDP packet from the neighbor within the aging time.

LLDP takes either of the following actions when neighbor aging occurs on an interface:

- **Block**—Blocks the interface. The `block` action places the data link layer protocol of the interface in **DOWN** state. In this state, the interface cannot transfer data packets. The data transfer capability is automatically recovered when the interface receives an LLDP packet.

- **Shutdown**—Shuts down the interface. The `shutdown` action places the interface in **LLDP DOWN** state. In this state, the interface can neither transfer data packets nor LLDP packets. You must manually execute the `undo lldp neighbor-protection aging` or `undo shutdown` command to bring up the interface.

To configure LLDP neighbor aging on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 or Layer 3 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable LLDP neighbor aging on the interface.</td>
<td>`lldp neighbor-protection aging { block</td>
</tr>
</tbody>
</table>

Configuring DCBX

Data Center Ethernet (DCE), also known as Converged Enhanced Ethernet (CEE), is enhancement and expansion of traditional Ethernet local area networks for use in data centers. DCE uses the Data Center Bridging Exchange Protocol (DCBX) to negotiate and remotely configure the bridge capability of network elements.

DCBX has the following self-adaptable versions:

- 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).

DCBX offers the following functions:

- Discovers the peer devices’ capabilities and determines whether devices at both ends support these capabilities.
- Detects configuration errors on peer devices.
- Remotely configures the peer device if the peer device accepts the configuration.

**NOTE:**

HPE devices support only the remote configuration feature.
DCBX enables lossless packet transmission on DCE networks.

As shown in Figure 97, DCBX applies to an FCoE-based data center network, and operates on an access switch. DCBX enables the switch to control the server or storage adapter, and simplifies the configuration and guarantees configuration consistency. DCBX extends LLDP by using the IEEE 802.1 organizationally specific TLVs (DCBX TLVs) to transmit DCBX data, including:

- In DCBX Rev 1.00 and DCBX Rev 1.01:
  - Application Protocol (APP).
  - Enhanced Transmission Selection (ETS).
  - Priority-based Flow Control (PFC).
- In IEEE Std 802.1Qaz-2011:
  - ETS Configuration.
  - ETS Recommendation.
  - PFC.
  - APP.

HPE devices can send these types of DCBX information to a server or storage adapter supporting FCoE. However, HPE devices cannot accept these types of DCBX information.

DCBX configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling LLDP and DCBX TLV advertising</td>
</tr>
<tr>
<td>(Required.) Setting the DCBX version</td>
</tr>
<tr>
<td>(Required.) Configuring APP parameters</td>
</tr>
<tr>
<td>(Required.) Configuring ETS parameters</td>
</tr>
<tr>
<td>• Configuring the 802.1p-to-local priority mapping</td>
</tr>
<tr>
<td>• Configuring group-based WRR queuing</td>
</tr>
<tr>
<td>(Required.) Configuring PFC parameters</td>
</tr>
</tbody>
</table>

Enabling LLDP and DCBX TLV advertising

To enable the device to advertise APP, ETS, and PFC data through an interface, perform the following tasks:

- Enable LLDP globally.
- Enable LLDP and DCBX TLV advertising on the interface.

To enable LLDP and DCBX TLV advertising:
### Setting the DCBX version

When you set the DCBX version, follow these restrictions and guidelines:

- For DCBX to work correctly, configure the same DCBX version on the local port and peer port. As a best practice, configure the highest version supported on both ends. IEEE Std 802.1Qaz-2011, DCBX Rev 1.01, and DCBX Rev 1.00 are in descending order.
- After the configuration, LLDP frames sent by the local port carry information about the configured DCBX version. The local port and peer port do not negotiate the DCBX version.
- When the DCBX version is autonegotiated, the version IEEE Std 802.1Qaz-2011 is preferably negotiated.

To set the DCBX version:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the DCBX version.</td>
<td>dcbx version { rev100</td>
<td>rev101</td>
</tr>
</tbody>
</table>

### Configuring APP parameters

The device negotiates with the server adapter by using the APP parameters to achieve the following purposes:

- Control the 802.1p priority values of the protocol packets that the server adapter sends.
- Identify traffic based on the 802.1p priority values.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the APP parameters.</td>
<td>app { 802.1p</td>
<td>ip</td>
</tr>
</tbody>
</table>
For example, the device can use the APP parameters to negotiate with the server adapter to set 802.1p priority 3 for all FCoE and FIP frames. When the negotiation succeeds, all FCoE and FIP frames that the server adapter sends to the device carry the 802.1p priority 3.

**Configuration restrictions and guidelines**

When you configure APP parameters, follow these restrictions and guidelines:

- An Ethernet frame header ACL identifies application protocol packets by frame type.
- An IPv4 advanced ACL identifies application protocol packets by TCP/UDP port number.
- DCBX Rev 1.00 identifies application protocol packets only by frame type and advertises only TLVs with frame type 0x8906 (FCoE).
- DCBX Rev 1.01 has the following attributes:
  - Supports identifying application protocol packets by both frame type and TCP/UDP port number.
  - Does not restrict the frame type or TCP/UDP port number for advertising TLVs.
  - Can advertise up to 77 TLVs according to the remaining length of the current packet.
- In a QoS policy, you can configure multiple class-behavior associations. A packet might be configured with multiple 802.1p priority marking or mapping actions, and the one configured first takes effect.

**Configuration procedure**

To configure APP parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an ACL and enter ACL view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create an Ethernet frame header ACL and enter ACL view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>acl mac { acl-number</td>
<td>name acl-name } [ match-order { auto</td>
</tr>
<tr>
<td></td>
<td>Create an IPv4 advanced ACL and enter ACL view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>acl advanced { acl-number</td>
<td>name acl-name } [ match-order { auto</td>
</tr>
<tr>
<td>3.</td>
<td>Create a rule for the ACL.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For the Ethernet frame header ACL:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rule [ rule-id ] permit type protocol-type ffff</td>
<td>Create rules according to the type of the ACL previously created.</td>
</tr>
<tr>
<td></td>
<td>For the IPv4 advanced ACL:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rule [ rule-id ] permit { tcp</td>
<td>udp } destination-port eq port</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Create a class, specify the operator of the class as OR, and enter class view.</td>
<td>traffic classifier classifier-name operator or</td>
</tr>
<tr>
<td>6.</td>
<td>Use the specified ACL as the match criterion of the class.</td>
<td>if-match acl acl-number</td>
</tr>
<tr>
<td>7.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>8.</td>
<td>Create a traffic behavior and enter traffic behavior view.</td>
<td>traffic behavior behavior-name</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>9.</td>
<td>Configure the behavior to mark packets with an 802.1p priority.</td>
<td>remark dot1p 8021p</td>
</tr>
<tr>
<td>10.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>11.</td>
<td>Create a QoS policy and enter QoS policy view.</td>
<td>qos policy policy-name</td>
</tr>
<tr>
<td>12.</td>
<td>Associate the class with the traffic behavior in the QoS policy, and apply the association to DCBX.</td>
<td>classifier classifier-name behavior behavior-name mode dcbx</td>
</tr>
<tr>
<td>13.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>14.</td>
<td>Apply the QoS policy.</td>
<td></td>
</tr>
</tbody>
</table>

- To the outgoing traffic of all ports:
  - qos apply policy policy-name global outbound
- To the outgoing traffic of a Layer 2 Ethernet interface:
  - Enter Layer 2 Ethernet interface view:
    - interface interface-type interface-number
  - Apply the QoS policy to the outgoing traffic:
    - qos apply policy policy-name outbound

For more information about the acl, rule, traffic classifier, if-match, traffic behavior, remark dot1p, qos policy, classifier behavior, qos apply policy global, and qos apply policy commands, see ACL and QoS Command Reference.

### Configuring ETS parameters

ETS provides committed bandwidth. To avoid packet loss caused by congestion, the device performs the following operations:

- Uses ETS parameters to negotiate with the server adapter.
- Controls the server adapter's transmission speed of the specified type of traffic.
- Guarantees that the transmission speed is within the committed bandwidth of the interface.

To configure ETS parameters, you must configure the 802.1p-to-local priority mapping and group-based WRR queuing.

#### Configuring the 802.1p-to-local priority mapping

You can configure the 802.1p-to-local priority mapping either in the MQC method or in the priority mapping table method. If you configure the 802.1p-to-local priority mapping in both methods, the configuration made in the MQC method applies.

To configure the 802.1p-to-local priority mapping in the MQC method:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a traffic class, specify the operator of the class as</td>
<td>traffic classifier classifier-name operator or</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3. OR, and enter class view.</td>
<td>if-match service-dot1p 8021p-list</td>
<td>By default, no match criterion is configured for the class to match packets.</td>
</tr>
<tr>
<td>4. Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>5. Create a traffic behavior and enter traffic behavior view.</td>
<td>traffic behavior behavior-name</td>
<td>By default, no traffic behavior exists.</td>
</tr>
<tr>
<td>6. Configure the behavior to mark packets with the specified local precedence value.</td>
<td>remark local-precedence local-precedence</td>
<td>By default, no local precedence marking action is configured.</td>
</tr>
<tr>
<td>7. Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>8. Create a QoS policy and enter QoS policy view.</td>
<td>qos policy policy-name</td>
<td>By default, no policy exists.</td>
</tr>
<tr>
<td>9. Associate the class with the traffic behavior in the QoS policy, and apply the association to DCBX.</td>
<td>classifier classifier-name behavior behavior-name mode dcbx</td>
<td>By default, no class-behavior association exists.</td>
</tr>
</tbody>
</table>

For more information about the **traffic classifier**, **if-match**, **traffic behavior**, **remark local-precedence**, **qos policy**, and **classifier behavior** commands, see [ACL and QoS Command Reference](#).

To configure the 802.1p priority mapping in the priority mapping table method:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter 802.1p-to-local priority mapping table view.</td>
<td>qos map-table dot1p-lp</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Configure the priority mapping table to map the specified 802.1p priority values to a local precedence value.</td>
<td>import import-value-list export export-value</td>
<td>For information about the default priority mapping tables, see <a href="#">ACL and QoS Configuration Guide</a>.</td>
</tr>
</tbody>
</table>

For more information about the **qos map-table**, **qos map-table color**, and **import** commands, see [ACL and QoS Command Reference](#).

**Configuring group-based WRR queuing**

You can configure group-based WRR queuing to allocate bandwidth.

To configure group-based WRR queuing:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable WRR queuing.</td>
<td>qos wrr byte-count</td>
<td>By default, byte-count WRR queuing is enabled on an interface.</td>
</tr>
<tr>
<td>4. Configure a queue.</td>
<td>• Add a queue to WRR priority group</td>
<td>Use one or both commands.</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
1. | 1 and configure the scheduling weight for the queue: **qos wrr queue-id group 1 byte-count schedule-value**<br>• Configure a queue to use SP queuing: **qos wrr queue-id group sp** | N/A

For more information about the **qos wrr**, **qos wrr byte-count**, and **qos wrr group sp** commands, see *ACL and QoS Command Reference*.

### Configuring PFC parameters

To prevent packets with an 802.1p priority value from being dropped, enable PFC for the 802.1p priority value. This feature reduces the sending rate of packets carrying this priority when network congestion occurs.

The device uses PFC parameters to negotiate with the server adapter and to enable PFC for the specified 802.1p priorities on the server adapter.

To configure PFC parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable PFC in auto mode on the Ethernet interface.</td>
<td>priority-flow-control auto</td>
</tr>
<tr>
<td>4.</td>
<td>Enable PFC for the specified 802.1p priorities.</td>
<td>priority-flow-control no-drop dot1p dot1p-list</td>
</tr>
</tbody>
</table>

For more information about the **priority-flow-control** and **priority-flow-control no-drop dot1p** commands, see *Interface Command Reference*.

### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet interface view, management Ethernet interface view, Layer</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>lldp source-mac vlan vlan-id</td>
<td>By default, the source MAC address of LLDP frames is the MAC address of the Layer 3 Ethernet interface. The specified VLAN ID is used as the subnumber element of the Layer 3 Ethernet subinterface number interface-number.subnumber.</td>
</tr>
</tbody>
</table>

### Setting the source MAC address of LLDP frames to the MAC address of a Layer 3 Ethernet subinterface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>lldp source-mac vlan vlan-id</td>
<td>By default, the source MAC address of LLDP frames is the MAC address of the Layer 3 Ethernet interface. The specified VLAN ID is used as the subnumber element of the Layer 3 Ethernet subinterface number interface-number.subnumber.</td>
</tr>
</tbody>
</table>
Enabling the device to generate ARP or ND entries for received management address LLDP TLVs

This feature enables the device to generate an ARP or ND entry for a received LLDP frame that carries a management address TLV. The ARP or ND entry contains the management address and the source MAC address of the frame.

You can enable the device to generate both ARP and ND entries. If the management address TLV contains an IPv4 address, the device generates an ARP entry. If the management address TLV contains an IPv6 address, the device generates an ND entry.

To enable the device to generate an ARP or ND entry for a received management address LLDP TLV:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the device to generate an ARP or ND entry for a management address LLDP TLV received on the interface.</td>
<td>lldp management-address { arp-learning</td>
</tr>
</tbody>
</table>

Displaying and maintaining LLDP

Execute display commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display local LLDP information.</td>
<td>display lldp local-information [ global</td>
</tr>
<tr>
<td>Display the information contained in the LLDP TLVs sent from neighboring devices.</td>
<td>display lldp neighbor-information [ [ [ interface interface-type interface-number ] [ agent { nearest-bridge</td>
</tr>
<tr>
<td>Display LLDP statistics.</td>
<td>display lldp statistics [ global</td>
</tr>
<tr>
<td>Display LLDP status of a port.</td>
<td>display lldp status [ interface interface-type interface-number ] [ agent { nearest-bridge</td>
</tr>
<tr>
<td>Display types of advertisable optional LLDP TLVs.</td>
<td>display lldp tlv-config [ interface interface-type interface-number ] [ agent { nearest-bridge</td>
</tr>
</tbody>
</table>
LLDP configuration examples

Basic LLDP configuration example

Network requirements

As shown in Figure 98, enable LLDP globally on Switch A and Switch B to perform the following tasks:

- Monitor the link between Switch A and Switch B on the NMS.
- Monitor the link between Switch A and the MED device on the NMS.

Figure 98 Network diagram

```
  NMS
  
  XGE1/0/1
  MED
  
  Switch A
  XGE1/0/1
  
  XGE1/0/2
  
  Switch B
```

Configuration procedure

1. Configure Switch A:
   
   ```
   # Enable LLDP globally.
   <SwitchA> system-view
   [SwitchA] lldp global enable
   # Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
   # Set the LLDP operating mode to Rx on Ten-GigabitEthernet 1/0/1.
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp admin-status rx
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   # Enable LLDP on Ten-GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.
   [SwitchA] interface ten-gigabitethernet 1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] lldp enable
   # Set the LLDP operating mode to Rx on Ten-GigabitEthernet 1/0/2.
   [SwitchA-Ten-GigabitEthernet1/0/2] lldp admin-status rx
   [SwitchA-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure Switch B:
   
   ```
   # Enable LLDP globally.
   <SwitchB> system-view
   [SwitchB] lldp global enable
   # Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] lldp enable
   # Set the LLDP operating mode to Tx on Ten-GigabitEthernet 1/0/1.
   [SwitchB-Ten-GigabitEthernet1/0/1] lldp admin-status tx
   ```
Verifying the configuration

# Verify the following items:

- Ten-GigabitEthernet 1/0/1 of Switch A connects to a MED device.
- Ten-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 max credit : 5
Hold multiplier : 4
Reinit delay : 2s
Trap interval : 30s
Fast start times : 4

LLDP status information of port 1 [Ten-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 status information of port 2 [Ten-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 Ten-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 max credit : 5
Hold multiplier : 4
Reinit delay : 2s
Trap interval : 30s
Fast start times : 4
LLDP status information of port 1 [Ten-GigabitEthernet1/0/1]:

LLDP agent nearest-bridge:
Port status of LLDP : Enable
Admin status : Rx_Only
Trap flag : No
MED trap flag : No
Polling interval : 0s
Number of LLDP neighbors : 1
Number of MED neighbors : 1
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP : Enable
Admin status : Disable
Trap flag : No
MED trap flag : No
Polling interval : 0s
Number of LLDP neighbors : 0
Number of MED neighbors : 0
Number of CDP neighbors : 0
Number of sent optional TLV : 1
Number of received unknown TLV : 0

LLDP status information of port 2 [Ten-GigabitEthernet1/0/2]:

LLDP agent nearest-bridge:
Port status of LLDP : Enable
Admin status : Rx_Only
Trap flag : No
MED trap flag : No
Polling interval : 0s
Number of LLDP neighbors : 0
Number of MED neighbors : 0
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP : Enable
Admin status : Disable
Trap flag : No
MED trap flag : No
Polling interval : 0s
Number of LLDP neighbors : 0
Number of MED neighbors : 0
Number of CDP neighbors : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0

CDP-compatible LLDP configuration example

Network requirements

As shown in Figure 99, Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone, which sends 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 operations:

- Confines the voice traffic to the voice VLAN.
- Isolates the voice traffic from other types of traffic.

Figure 99 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to trunk, and enable voice VLAN on them.
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
   [SwitchA-Ten-GigabitEthernet1/0/1] voice vlan 2 enable
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   [SwitchA] interface ten-gigabitethernet 1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
   [SwitchA-Ten-GigabitEthernet1/0/2] voice vlan 2 enable
   [SwitchA-Ten-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 Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable

# Configure LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/1.
[SwitchA-Ten-GigabitEthernet1/0/1] lldp admin-status txrx

# Configure CDP-compatible LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/1.
[SwitchA-Ten-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-Ten-GigabitEthernet1/0/1] quit

# Enable LLDP on Ten-GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] lldp enable

# Configure LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/2.
[SwitchA-Ten-GigabitEthernet1/0/2] lldp admin-status txrx

# Configure CDP-compatible LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/2.
[SwitchA-Ten-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-Ten-GigabitEthernet1/0/2] quit

Verifying the configuration

# Verify that Switch A has completed the following operations:
- Discovering the IP phones connected to Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.
- Obtaining IP phone information.

[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[Ten-GigabitEthernet1/0/1]:
  CDP neighbor index : 1
  Chassis ID          : SEP00141C8CDBFE
  Port ID             : Port 1
  Software version    : P0030301MFG2
  Platform            : Cisco IP Phone 7960
  Duplex              : Full

CDP neighbor-information of port 2[Ten-GigabitEthernet1/0/2]:
  CDP neighbor index : 2
  Chassis ID          : SEP00141C8CDBFF
  Port ID             : Port 1
  Software version    : P0030301MFG2
  Platform            : Cisco IP Phone 7960
  Duplex              : Full

DCBX configuration example

Network requirements

As shown in Figure 100, Ten-GigabitEthernet 1/0/1 of the access switch (Switch A) connects to the FCoE adapter of the data center server (DC server).
Configure Switch A to implement lossless FCoE and FIP frame transmission to DC server.

**NOTE:**
In this example, both Switch A and the DC server support DCBX Rev 1.01.

**Figure 100 Network diagram**

Configuration procedure

1. **Enable LLDP and DCBX TLV advertising:**
   
   # Enable LLDP globally.
   ```
   <SwitchA> system-view
   [SwitchA] lldp global enable
   # Enable LLDP and DCBX TLV advertising on Ten-GigabitEthernet 1/0/1.
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
   ```

2. **Set the DCBX version to Rev. 1.01 on Ten-GigabitEthernet 1/0/1.**
   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] dcbx version rev101
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

3. **Configure APP parameters:**
   
   # Create Ethernet frame header ACL 4000.
   ```
   [SwitchA] acl mac 4000
   # Configure ACL 4000 to permit FCoE frames (frame type is 0x8906) and FIP frames (frame type is 0x8914) to pass through.
   [SwitchA-acl-mac-4000] rule permit type 8906 ffff
   [SwitchA-acl-mac-4000] rule permit type 8914 ffff
   [SwitchA-acl-mac-4000] quit
   # Create a class named app_c, set the operator of the class to OR, and use ACL 4000 as the match criterion of the class.
   [SwitchA] traffic classifier app_c operator or
   [SwitchA-classifier-app_c] if-match acl 4000
   [SwitchA-classifier-app_c] quit
   # Create a traffic behavior named app_b, and configure the traffic behavior to mark packets with 802.1p priority value 3.
   [SwitchA] traffic behavior app_b
   [SwitchA-behavior-app_b] remark dot1p 3
   [SwitchA-behavior-app_b] quit
   # Create a QoS policy named plcy, associate class app_c with traffic behavior app_b in the QoS policy, and apply the association to DCBX.
   [SwitchA] qos policy plcy
   [SwitchA-qospolicy-plcy] classifier app_c behavior app_b mode dcbx
   ```
[SwitchA-qospolicy-plcy] quit

# Apply QoS policy plcy to the outgoing traffic of Ten-GigabitEthernet 1/0/1.

[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy plcy outbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit

4. Configure ETS parameters:
   # Configure the 802.1p-to-local priority mapping table to map 802.1p priority value 3 to local precedence 3. (This is the default mapping table. You can modify this configuration as needed.)

[SwitchA] qos map-table dot1p-lp
[SwitchA-maptbl-dot1p-lp] import 3 export 3
[SwitchA-maptbl-dot1p-lp] quit

# Enable byte-count WRR queuing on Ten-GigabitEthernet 1/0/1, and configure queue 3 on the interface to use SP queuing.

[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 3 group sp

5. Configure PFC:
   # Enable PFC in auto mode on Ten-GigabitEthernet 1/0/1.

[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto

# Enable PFC for 802.1 priority 3.

[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3

Verifying the configuration
# Display the data exchange result on the DC server through the software interface. This example uses the data exchange result for a QLogic adapter on the DC server.

----------------------------------------
DCBX Parameters Details for CNA Instance 0 - QLE8142
----------------------------------------

Mon May 17 10:00:50 2010

DCBX TLV (Type-Length-Value) Data
----------------------------------------
DCBX Parameter Type and Length
   DCBX Parameter Length: 13
   DCBX Parameter Type: 2

DCBX Parameter Information
   Parameter Type: Current
   Pad Byte Present: Yes
   DCBX Parameter Valid: Yes
   Reserved: 0

DCBX Parameter Data
   Priority Group ID of Priority 1: 0
   Priority Group ID of Priority 0: 2
   Priority Group ID of Priority 3: 15
   Priority Group ID of Priority 2: 1
Priority Group ID of Priority 5: 5
Priority Group ID of Priority 4: 4

Priority Group ID of Priority 7: 7
Priority Group ID of Priority 6: 6

Priority Group 0 Percentage: 2
Priority Group 1 Percentage: 4
Priority Group 2 Percentage: 6
Priority Group 3 Percentage: 0
Priority Group 4 Percentage: 10
Priority Group 5 Percentage: 18
Priority Group 6 Percentage: 27
Priority Group 7 Percentage: 31

Number of Traffic Classes Supported: 8

DCBX Parameter Information

Parameter Type: Remote
Pad Byte Present: Yes
DCBX Parameter Valid: Yes
Reserved: 0

DCBX Parameter Data

Priority Group ID of Priority 1: 0
Priority Group ID of Priority 0: 2

Priority Group ID of Priority 3: 15
Priority Group ID of Priority 2: 1

Priority Group ID of Priority 5: 5
Priority Group ID of Priority 4: 4

Priority Group ID of Priority 7: 7
Priority Group ID of Priority 6: 6

Priority Group 0 Percentage: 2
Priority Group 1 Percentage: 4
Priority Group 2 Percentage: 6
Priority Group 3 Percentage: 0
Priority Group 4 Percentage: 10
Priority Group 5 Percentage: 18
Priority Group 6 Percentage: 27
Priority Group 7 Percentage: 31

Number of Traffic Classes Supported: 8
DCBX Parameter Information

Parameter Type: Local
Pad Byte Present: Yes
DCBX Parameter Valid: Yes
Reserved: 0

DCBX Parameter Data

Priority Group ID of Priority 1: 0
Priority Group ID of Priority 0: 0
Priority Group ID of Priority 3: 1
Priority Group ID of Priority 2: 0
Priority Group ID of Priority 5: 0
Priority Group ID of Priority 4: 0
Priority Group ID of Priority 7: 0
Priority Group ID of Priority 6: 0

Priority Group 0 Percentage: 50
Priority Group 1 Percentage: 50
Priority Group 2 Percentage: 0
Priority Group 3 Percentage: 0
Priority Group 4 Percentage: 0
Priority Group 5 Percentage: 0
Priority Group 6 Percentage: 0
Priority Group 7 Percentage: 0

Number of Traffic Classes Supported: 2

The output shows that the DC server will use SP queuing (priority group ID 15) for 802.1p priority 3.

DCBX Parameter Type and Length

DCBX Parameter Length: 2
DCBX Parameter Type: 3

DCBX Parameter Information

Parameter Type: Current
Pad Byte Present: No
DCBX Parameter Valid: Yes
Reserved: 0

DCBX Parameter Data

PFC Enabled on Priority 0: No
PFC Enabled on Priority 1: No
PFC Enabled on Priority 2: No
PFC Enabled on Priority 3: Yes
PFC Enabled on Priority 4: No
PFC Enabled on Priority 5: No
PFC Enabled on Priority 6: No
PFC Enabled on Priority 7: No

Number of Traffic Classes Supported: 6

DCBX Parameter Information

Parameter Type: Remote
Pad Byte Present: No
DCBX Parameter Valid: Yes
Reserved: 0

DCBX Parameter Data

PFC Enabled on Priority 0: No
PFC Enabled on Priority 1: No
PFC Enabled on Priority 2: No
PFC Enabled on Priority 3: Yes
PFC Enabled on Priority 4: No
PFC Enabled on Priority 5: No
PFC Enabled on Priority 6: No
PFC Enabled on Priority 7: No

Number of Traffic Classes Supported: 6

DCBX Parameter Information

Parameter Type: Local
Pad Byte Present: No
DCBX Parameter Valid: Yes
Reserved: 0

DCBX Parameter Data

PFC Enabled on Priority 0: No
PFC Enabled on Priority 1: No
PFC Enabled on Priority 2: No
PFC Enabled on Priority 3: Yes
PFC Enabled on Priority 4: No
PFC Enabled on Priority 5: No
PFC Enabled on Priority 6: No
PFC Enabled on Priority 7: No

Number of Traffic Classes Supported: 1

The output shows that the DC server will use PFC for 802.1p priority 3.
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 or drop them.

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 101, 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 101 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.
- DLDL.
- EOAM.
- GVRP.
- LACP.
- LLDP.
- MVRP.
- PAgP.
• PVST.
• STP (including STP, RSTP, and MSTP).
• UDLD.
• VTP.

L2PT operating mechanism

As shown in Figure 102, 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 2 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 102 L2PT operating mechanism

For example, as shown in Figure 103, 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:
   - 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.
   - 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.
L2PT configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling L2PT</td>
</tr>
<tr>
<td>(Optional.) Setting the destination multicast MAC address for tunneled packets</td>
</tr>
</tbody>
</table>

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.
- Do not enable L2PT on a port that is going to join a service loopback group. All configuration is removed after the port joins the group.
- 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>Enter Layer 2 Ethernet interface view:</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Set the destination multicast MAC address for tunneled packets.</td>
<td>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.</td>
</tr>
</tbody>
</table>
L2PT configuration examples

Configuring L2PT for STP

Network requirements

As shown in Figure 104, 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 104 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 Ten-GigabitEthernet 1/0/1 as an access port and assign the port to VLAN 2.
   [PE1] interface ten-gigabitethernet 1/0/1
   [PE1-Ten-GigabitEthernet1/0/1] port access vlan 2
   # Disable STP and enable L2PT for STP on Ten-GigabitEthernet 1/0/1.
   [PE1-Ten-GigabitEthernet1/0/1] undo stp enable
   [PE1-Ten-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
   [PE1-Ten-GigabitEthernet1/0/1] quit
   # Configure Ten-GigabitEthernet 1/0/2 connected to the service provider network as a trunk port, and assign the port to all VLANs.
   [PE1] interface ten-gigabitethernet 1/0/2
   [PE1-Ten-GigabitEthernet1/0/2] port link-type trunk
2. Configure PE 2 in the same way PE 1 is configured. (Details not shown.)

Verifying the configuration

```plaintext
[CE2] display stp root
MST ID  Root Bridge ID     ExtPathCost IntPathCost Root Port
0       32768.00e0-fc02-5800 0           0

[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 105, 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 on CE 1 to form aggregate links with Ten-GigabitEthernet 1/0/1 and Ten-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 105 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 Ten-GigabitEthernet 1/0/1 and Ten-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 Ten-GigabitEthernet 1/0/1 and Ten-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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to Bridge-Aggregation 1.
   
   [CE1] interface ten-gigabitethernet 1/0/1
   
   [CE1-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   
   [CE1-Ten-GigabitEthernet1/0/1] quit
   
   [CE1] interface ten-gigabitethernet 1/0/2
   
   [CE1-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
   
   [CE1-Ten-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 Ten-GigabitEthernet 1/0/1 as a trunk port, assign the port to VLAN 2, and set the PVID to VLAN 2.
   
   [PE1] interface ten-gigabitethernet 1/0/1
   
   [PE1-Ten-GigabitEthernet1/0/1] port link-mode bridge
   
   [PE1-Ten-GigabitEthernet1/0/1] port link-type trunk
   
   [PE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 2
   
   [PE1-Ten-GigabitEthernet1/0/1] port trunk pvid vlan 2
   
   # Enable QinQ on Ten-GigabitEthernet 1/0/1.
   
   [PE1-Ten-GigabitEthernet1/0/1] qinq enable
   
   # Enable L2PT for LACP on Ten-GigabitEthernet 1/0/1.
   
   [PE1-Ten-GigabitEthernet1/0/1] l2protocol lacp tunnel dot1q
   
   [PE1-Ten-GigabitEthernet1/0/1] quit
   
   # Configure Ten-GigabitEthernet 1/0/2 as a trunk port, assign the port to VLAN 3, and set the PVID to VLAN 3.
   
   [PE1] interface ten-gigabitethernet 1/0/2
   
   [PE1-Ten-GigabitEthernet1/0/2] port link-mode bridge
   
   [PE1-Ten-GigabitEthernet1/0/2] port link-type trunk
   
   [PE1-Ten-GigabitEthernet1/0/2] port trunk permit vlan 3
   
   [PE1-Ten-GigabitEthernet1/0/2] port trunk pvid vlan 3
   
   # Enable QinQ on Ten-GigabitEthernet 1/0/2.
   
   [PE1-Ten-GigabitEthernet1/0/2] qinq enable
# Enable L2PT for LACP on Ten-GigabitEthernet 1/0/2.

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

Ten-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)

Ten-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
Ten-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)

Ten-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 service loopback groups

A service loopback group contains one or multiple Ethernet ports for looping packets sent out by the device back to the device. This feature must work with other features, such as GRE.

A service loopback group provides one of the following services:
- **Tunnel**—Supports unicast tunnel traffic.
- **Multicast tunnel**—Supports multicast tunnel traffic.
- **Multiport**—Supports multiport ARP traffic.
- **VSI gateway**—Supports VSI gateway traffic.

You can configure only one service loopback group for a service type. However, you can use one service loopback group with multiple features.

Member ports in a service loopback group are load balanced.

Configuration procedure

Follow these guidelines when you configure a service loopback group:
- Make sure the ports you are assigning to a service loopback group meet the following requirements:
  - The ports are not used for any other purposes. The configuration on a port is removed when it is assigned to a service loopback group.
  - The ports support the service type of the service loopback group and are not members of any other service loopback group.
- You cannot change the service type of a service loopback group.
- Do not delete a service loopback group that is being used by a feature.
- To avoid IRF split, do not assign a port to a service loopback group if that port is the only IRF physical interface of an IRF port.
- For correct traffic processing, make sure a service loopback group has a minimum of one member port when it is being used by a feature.

To configure a service loopback group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Create a service loopback group and specify its service type.</td>
<td><strong>service-loopback group</strong> <strong>group-id</strong> <strong>type</strong> { { multicast-tunnel</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><strong>interface</strong> <strong>interface-type</strong> <strong>interface-number</strong></td>
</tr>
<tr>
<td>4.</td>
<td>Assign the port to the service loopback group.</td>
<td><strong>port service-loopback group</strong> <strong>group-id</strong></td>
</tr>
</tbody>
</table>
Displaying and maintaining service loopback groups

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about service loopback groups.</td>
<td><code>display service-loopback group [group-id]</code></td>
</tr>
</tbody>
</table>

Service loopback group configuration example

Network requirements

All Ethernet ports on Device A support the tunnel service. Assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to a service loopback group to loop GRE packets sent out by the device back to the device.

Configuration procedure

# Create service loopback group 1, and specify its service type as tunnel.
<DeviceA> system-view
[DeviceA] service-loopback group 1 type tunnel

# Assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to service loopback group 1.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port service-loopback group 1
All configurations on the interface will be lost. Continue?[Y/N]: y
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port service-loopback group 1
All configurations on the interface will be lost. Continue?[Y/N]: y
[DeviceA-Ten-GigabitEthernet1/0/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
All configurations on the interface will be lost. Continue?[Y/N]: y
[DeviceA-Ten-GigabitEthernet1/0/3] quit

# Create the interface Tunnel 1 and set it to GRE mode. The interface will automatically use service loopback group 1.
[DeviceA] interface tunnel 1 mode gre
[DeviceA-Tunnel1]
Configuring cut-through forwarding

A cut-through forwarding-enabled device forwards a frame after it receives the first 64 bytes of the frame. This feature reduces the transmission time of a frame and enhances forwarding performance.

To configure cut-through forwarding:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>cut-through enable</td>
<td>By default, cut-through forwarding is disabled.</td>
</tr>
</tbody>
</table>

**NOTE:**

A frame is forwarded before its CRC field is received, and thus CRC-error frames are forwarded instead of dropped.
Configuring DRNI

Overview

Distributed Resilient Network Interconnect (DRNI) virtualizes two physical devices into one system through multichassis link aggregation.

DRNI network model

As shown in Figure 106, DRNI virtualizes two devices into a distributed-relay (DR) system, which connects to the remote aggregation system through a multichassis aggregate link. To the remote aggregation system, the DR system is one device.

Figure 106 DRNI network model

The DR member devices are DR peers to each other. DRNI defines the following interface roles for each DR member device:

- **DR interface**—Layer 2 aggregate interface connected to the remote aggregation system. DR interfaces connected to the same remote aggregation system belong to one DR group. In Figure 106, Bridge-Aggregation 1 on Device A and Bridge-Aggregation 2 on Device B belong to the same DR group. DR interfaces in a DR group form a multichassis aggregate link.

- **Intra-portal port (IPP)**—Interface connected to the DR peer for internal control. Each DR member device has only one IPP. The IPPs of the DR member devices transmit DRNI protocol packets through the intra-portal link (IPL) established between them. A DR system has only one IPL.
DR member devices use a keepalive link to monitor each other's state. For more information about the keepalive mechanism, see "Keepalive and failover mechanism."

Roles of DR member devices

For features that require centralized traffic processing (for example, spanning tree), a DR member device is assigned the primary or secondary role based on its DR role priority. The secondary DR device passes the traffic of those features to the primary DR device for processing. If the DR member devices in a DR system have the same DR role priority, the device with the lower bridge MAC address is assigned the primary role.

DRCP

DRNI uses IEEE P802.1AX Distributed Relay Control Protocol (DRCP) for multichassis link aggregation. DRCP runs on the IPL and uses distributed relay control protocol data units (DRCPDUs) to advertise the DRNI configuration out of IPPs and DR interfaces.

DRCP operating mechanism

DRNI-enabled devices use DRCPDUs for the following purposes:

- Exchange DRCPDUs through DR interfaces to determine whether they can form a DR system.
- Exchange DRCPDUs through IPPs to negotiate the IPL state.

DRCP timeout timers

DRCP uses a timeout mechanism to specify the amount of time that an IPP or DR interface must wait to receive DRCPDUs before it determines that the peer interface is down. This timeout mechanism provides the following timer options:

- Short DRCP timeout timer, which is fixed at 3 seconds. If this timer is used, the peer interface sends one DRCPDU every second.
- Long DRCP timeout timer, which is fixed at 90 seconds. If this timer is used, the peer interface sends one DRCPDU every 30 seconds.

Short DRCP timeout timer enables the DR member devices to detect a peer interface down event more quickly than the long DRCP timeout timer. However, this benefit is at the expense of bandwidth and system resources.

Keepalive and failover mechanism

For the secondary DR device to monitor the state of the primary device, you must establish a Layer 3 keepalive link between the DR member devices.

The DR member devices periodically send keepalive packets over the keepalive link. The secondary DR device determines that the primary DR device is down if all the following conditions are met when the keepalive timeout timer expires:

- It has not received keepalive packets from the primary DR device. In this situation, the keepalive link is down.
- The IPL is down.

Then, the secondary DR device takes over.

If the keepalive link is down while the IPL is up, the DR member devices prompt you to check for keepalive link issues.
MAD mechanism

A multi-active collision occurs if the IPL goes down while the keepalive link is up. To avoid network issues, DRNI MAD shuts down all network interfaces on the secondary DR device except for the interfaces excluded from the MAD shutdown action. The interfaces excluded from the MAD shutdown action include:

- Interfaces excluded automatically by the system. The interfaces include IPPs, DR interfaces (available in R2612 and later), and management Ethernet interfaces.
- Interfaces excluded manually.

When the IPL comes up, the secondary DR device starts a delay timer and begins to restore entries (including MAC address entries and ARP entries) from the primary DR device. When the delay timer expires, the secondary DR device brings up all network interfaces.

**IMPORTANT:**

For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action by DRNI MAD. If the IPP is a tunnel interface, you must exclude the traffic outgoing interface for the tunnel from the shutdown action by DRNI MAD.

DR system setup process

As shown in Figure 107, two devices perform the following operations to form a DR system:

1. Send DRCPDUs over the IPL to each other and compare the DRCPDUs to determine the DR system stackability and device roles:
   - a. Compare the DR system settings. The devices can form a DR system if they have the same DR system MAC address and system priority and different DR system numbers.
   - b. Determine the device roles based on the DR role priority and the bridge MAC address.
   - c. Perform configuration consistency check. For more information, see "Configuration consistency check."

2. Send keepalive packets over the keepalive link to verify that the peer system is operating correctly.

3. Synchronize configuration data by sending DRCPDUs over the IPL. The configuration data includes MAC address entries and ARP entries.
Configuration consistency check

During DR system setup, DR member devices exchange the configuration and perform configuration consistency check to verify their consistency in the following configurations:

- **Type 1 configuration**—Settings that affect traffic forwarding of the DR system. If an inconsistency in type 1 configuration is detected, the secondary DR device shuts down its DR interfaces.

- **Type 2 configuration**—Settings that affect only service features. If an inconsistency in type 2 configuration is detected, the secondary DR device disables the affected service features, but it does not shut down its DR interfaces.

To prevent interface flapping, the DR system performs configuration consistency check when half the data restoration internal elapses.

**NOTE:**

The data restoration interval specifies the maximum amount of time for the secondary DR device to synchronize data with the primary DR device during DR system setup. For more information, see "Setting the data restoration interval."

**Type 1 configuration**

Type 1 configuration consistency check is performed both globally and on DR interfaces. Table 29 and Table 30 show settings that type 1 configuration contains.
Table 29 Global type 1 configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPP link type</td>
<td>IPP link type, which can be access, hybrid, or trunk.</td>
</tr>
<tr>
<td>PVID on the IPP</td>
<td>PVID on the IPP.</td>
</tr>
<tr>
<td>Spanning tree state</td>
<td>• Global spanning tree state.</td>
</tr>
<tr>
<td></td>
<td>• VLAN-specific spanning tree state.</td>
</tr>
<tr>
<td>Spanning tree mode</td>
<td>Spanning tree mode, including STP, RSTP, PVST, and MSTP.</td>
</tr>
<tr>
<td>MST region settings</td>
<td>• MST region name.</td>
</tr>
<tr>
<td></td>
<td>• MST region revision level.</td>
</tr>
<tr>
<td></td>
<td>• VLAN-to-MSTI mappings.</td>
</tr>
</tbody>
</table>

Table 30 DR interface type 1 configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation mode</td>
<td>Aggregation mode, including static and dynamic.</td>
</tr>
<tr>
<td>Spanning tree state</td>
<td>Interface-specific spanning tree state.</td>
</tr>
<tr>
<td>Link type</td>
<td>Interface link type, including access, hybrid, and trunk.</td>
</tr>
<tr>
<td>PVID</td>
<td>Interface PVID.</td>
</tr>
</tbody>
</table>

Type 2 configuration

Type 2 configuration consistency check is performed both globally and on DR interfaces. Table 31 and Table 32 show settings that type 2 configuration contains.

Table 31 Global type 2 configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN interfaces</td>
<td>Up VLAN interfaces of which the VLANs contain the IPP.</td>
</tr>
<tr>
<td>Passing tagged VLANs or passing PVID</td>
<td>VLANs of which the IPP forwards tagged traffic or PVID of which the IPP forwards traffic.</td>
</tr>
</tbody>
</table>

Table 32 DR interface type 2 configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing tagged VLANs</td>
<td>VLANs of which a DR interface forwards tagged traffic.</td>
</tr>
<tr>
<td>Passing untagged VLANs</td>
<td>VLANs of which a DR interface forwards untagged traffic.</td>
</tr>
</tbody>
</table>

DRNI failure handling mechanisms

DR interface failure handling mechanism

When the DR interface of one DR member device fails, the DR system forwards traffic through the other DR member device.

As shown in Figure 108, Device A and Device B form a DR system, to which Device C is attached through a multichassis aggregation. If traffic to Device C arrives at Device B after the DR interface connected Device B to Device C has failed, the DR system forwards the traffic as follows:

1. Device B sends the traffic to Device A over the IPL.
2. Device A forwards the downlink traffic received from the IPL to Device C. After the faulty DR interface comes up, Device B forwards traffic to Device C through the DR interface.

**Figure 108 DR interface failure handling mechanism**

As shown in **Figure 109**, multi-active collision occurs if the IPL goes down while the keepalive link is up. To avoid network issues, the secondary DR device sets all network interfaces to DRNI MAD DOWN state except for the interfaces excluded from the MAD shutdown action by DRNI.

In this situation, the primary DR device forwards all traffic for the DR system.

When the IPP comes up, the secondary DR device does not bring up the network interfaces immediately. Instead, it starts a delay timer and begins to recover data from the primary DR device. When the delay timer expires, the secondary DR device brings up all network interfaces.

**Figure 109 IPL failure handling mechanism**

**Device failure handling mechanism**

As shown in **Figure 110**, when the primary DR device fails, the secondary DR device takes over the primary role to forward all traffic for the DR system. When the faulty device recovers, it becomes the secondary DR device.

When the secondary DR device fails, the primary DR device forwards all traffic for the DR system.
Protocols and standards

IEEE P802.1AX-REV™/D4.4c, Draft Standard for Local and Metropolitan Area Networks

Configuration restrictions and guidelines

For DRNI to operate correctly, do not use DRNI on an IRF fabric. For more information about IRF, see Virtual Technologies Configuration Guide.

For the DR member devices to be identified as one DR system, you must configure the same DR system MAC address and DR system priority on them. You must assign different DR system numbers to the DR member devices.

For correct traffic forwarding, make sure the DR member devices are consistent in service feature settings.

When you configure a DR interface, follow these restrictions and guidelines:

- The `link-aggregation selected-port maximum` and `link-aggregation selected-port minimum` commands do not take effect on a DR interface.
- If you execute the `display link-aggregation verbose` command for a DR interface, the displayed system ID contains the DR system MAC address and the DR system priority.
- If the reference port is a member port of a DR interface, the `display link-aggregation verbose` command displays the reference port on both DR member devices.

For more information about Ethernet link aggregation, see Layer 2—LAN Switching Configuration Guide.

DRNI configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring DR system settings:</td>
</tr>
<tr>
<td>• Configuring the DR system MAC address</td>
</tr>
<tr>
<td>• Setting the DR system number</td>
</tr>
<tr>
<td>• Setting the DR system priority</td>
</tr>
<tr>
<td>(Optional.) Setting the DR role priority of the device</td>
</tr>
<tr>
<td>(Required.) Configuring DR keepalive settings:</td>
</tr>
</tbody>
</table>

Figure 110 Device failure handling mechanism
### Tasks at a glance

- **(Required.)** Excluding an interface from the shutdown action by DRNI MAD:
  - Excluding an interface from the shutdown action by DRNI MAD (Release 2609)
  - Excluding an interface from the shutdown action by DRNI MAD (R2612 and later)
- **(Required.)** Configuring DR keepalive packet parameters
- **(Optional.)** Setting the DR keepalive interval and timeout timer

- **(Required.)** Configuring a DR interface
- **(Optional.)** Specifying a Layer 2 aggregate interface or VXLAN tunnel interface as the IPP
- **(Optional.)** Disabling configuration consistency check
- **(Optional.)** Enabling the short DRCP timeout timer on the IPP or a DR interface
- **(Optional.)** Setting the keepalive hold timer for identifying the cause of IPL down events
- **(Required.)** Configuring DR system auto-recovery
- **(Optional.)** Setting the data restoration interval

### Configuring DR system settings

#### Configuring the DR system MAC address

**Configuration restrictions and guidelines**

⚠️ **CAUTION:**
Changing the DR system MAC address causes DR system split. When you perform this task on a live network, make sure you are fully aware of its impact.

The DR system MAC address uniquely identifies the DR system on the network. For the DR member devices to be identified as one DR system, you must configure the same DR system MAC address on them. As a best practice, use the bridge MAC address of one DR member device as the DR system MAC address.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the DR system MAC address.</td>
<td>drni system-mac mac-address</td>
</tr>
</tbody>
</table>

By default, the DR system MAC address is not configured.

#### Setting the DR system number

**Configuration restrictions and guidelines**

⚠️ **CAUTION:**
Changing the DR system number causes DR system split. When you perform this task on a live network, make sure you are fully aware of its impact.

You must assign different DR system numbers to the DR member devices in a DR system.
### Setting the DR system priority

#### About the DR system priority
A DR system uses its DR system priority as the system LACP priority to communicate with the remote aggregation system.

#### Configuration restrictions and guidelines

⚠️ **CAUTION:**
Changing the DR system priority causes DR system split. When you perform this task on a live network, make sure you are fully aware of its impact.

You must configure the same DR system priority for the DR member devices in a DR system.

#### Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the DR system number.</td>
<td><code>drni system-number system-number</code></td>
<td>By default, the DR system number is not set.</td>
</tr>
</tbody>
</table>

### Setting the DR role priority of the device

#### About the DR role priority
DRNI assigns the primary or secondary role to a DR member device based on its DR role priority. The smaller the priority value, the higher the priority. If the DR member devices in a DR system use the same DR role priority, the device with the lower bridge MAC address is assigned the primary role.

#### Restrictions and guidelines
To prevent a primary/secondary role switchover from causing network flapping, avoid changing the DR priority assignment after the DR system is established.

#### Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the DR role priority of the device.</td>
<td><code>drni role priority priority-value</code></td>
<td>By default, the DR role priority of the device is 32768.</td>
</tr>
</tbody>
</table>
Configuring DR keepalive settings

Configuration restrictions and guidelines for configuring DR keepalive settings

When you set up a keepalive link, follow these restrictions and guidelines:

- Use Layer 3 Ethernet interfaces or management Ethernet interfaces to set up the keepalive link.
- Make sure the two ends use the same keepalive settings. DR member devices check the peer keepalive settings for consistency. If an inconsistency is found, the device will prompt for configuration revision.

Excluding an interface from the shutdown action by DRNI MAD (Release 2609)

Configuration restrictions and guidelines

For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action by DRNI MAD. If the IPP is a tunnel interface, you must exclude the traffic outgoing interface for the tunnel from the shutdown action by DRNI MAD.

To view interfaces manually excluded from the MAD shutdown action, see the Excluded ports (user-configured) field in the output from the `display mad verbose` command. For more information about this command, see Virtual Technologies Command Reference.

To view interfaces automatically excluded from the MAD shutdown action, use the `display drni mad verbose` command.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>mad exclude interface interface-type interface-number</td>
<td>By default, DRNI MAD shuts down all network interfaces when detecting a multi-active collision, except for the interfaces automatically excluded by the system.</td>
</tr>
</tbody>
</table>

Excluding an interface from the shutdown action by DRNI MAD (R2612 and later)

Configuration restrictions and guidelines

For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action by DRNI MAD. If the IPP is a tunnel interface, you must exclude the traffic outgoing interface for the tunnel from the shutdown action by DRNI MAD.

To view interfaces manually or automatically excluded from the MAD shutdown action, use the `display drni mad verbose` command.

If an interface has been placed in DRNI MAD DOWN state, executing the `drni mad exclude interface` command cannot bring it up.
**Configuration procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Exclude an interface from the MAD shutdown action by DRNI.</td>
<td>drni mad exclude interface interface-type interface-number</td>
<td>By default, DRNI MAD shuts down all network interfaces when detecting a multi-active collision, except for the interfaces automatically excluded by the system.</td>
</tr>
</tbody>
</table>

**Configuring DR keepalive packet parameters**

**About DR keepalive packet parameters**

Perform this task to specify the parameters for sending DR keepalive packets, such as its source and destination IP addresses.

The device accepts only keepalive packets that are sourced from the specified destination IP address. The keepalive link goes down if the device receives keepalive packets sourced from any other IP address.

**Configuration restrictions and guidelines**

Make sure the DR member devices in a DR system use the same keepalive destination UDP port.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure DR keepalive packet parameters.</td>
<td>drni keepalive { ip</td>
<td>ipv6 } destination { ipv4-address</td>
</tr>
<tr>
<td>3. Configure DR keepalive packet parameters.</td>
<td>drni keepalive { ip</td>
<td>ipv6 } destination { ipv4-address</td>
</tr>
</tbody>
</table>
Setting the DR keepalive interval and timeout timer

About the DR keepalive interval and timeout timer

The device sends keepalive packets at the specified interval to its DR peer. If the device has not received a keepalive packet from the DR peer before the keepalive timeout timer expires, the device determines that the keepalive link is down.

Configuration restrictions and guidelines

The local DR keepalive timeout timer must be two times the DR keepalive interval of the peer at minimum.

Configure the same DR keepalive interval on the DR member devices in the DR system.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>drni keepalive interval interval [ timeout timeout ]</code></td>
<td>By default, the DR keepalive interval is 1000 milliseconds, and the DR keepalive timeout timer is 5 seconds.</td>
</tr>
</tbody>
</table>

Configuring a DR interface

Configuration restrictions and guidelines

The device can have multiple DR interfaces. However, you can assign a Layer 2 aggregate interface to only one DR group.

A Layer 2 aggregate interface cannot operate as both IPP and DR interface.

To improve the forwarding efficiency, exclude the DR interface on the secondary DR device from the shutdown action by DRNI MAD. This action enables the DR interface to forward traffic immediately after a multi-active collision is removed without having to wait for the secondary DR device to complete entry restoration.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>interface bridge-aggregation interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><code>port drni group group-id</code></td>
<td>By default, an aggregate interface does not belong to a DR group.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Exclude the DR interface from the shutdown action by DRNI MAD.</td>
<td>By default, a DR interface is shut down when a multi-active collision is detected.</td>
</tr>
</tbody>
</table>
Specifying a Layer 2 aggregate interface or VXLAN tunnel interface as the IPP

Configuration restrictions and guidelines

A DR member device can have only one IPP. A Layer 2 aggregate interface or VXLAN tunnel interface cannot operate as both IPP and DR interface.

Do not associate a VXLAN tunnel interface with VXLANs if you use it as the IPP. You can use a VXLAN tunnel interface as an IPP only in an EVPN network. For more information about EVPN, see EVPN Configuration Guide.

To prevent data synchronization failure, you must set the same maximum jumbo frame length on the IPPs of the DR member devices. For more information about jumbo frames, see "Configuring Ethernet link aggregation."

Do not use the MAC address of a remote MEP for CFD tests on IPPs. These tests cannot work on IPPs. For more information about CFD, see High Availability Configuration Guide.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view. | • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number  
• Enter VXLAN tunnel interface view: interface tunnel number | N/A |
| 3.   | Specify the aggregate interface as the IPP. | port drni intra-portal-port port-id | By default, an aggregate interface is not the IPP. |

Disabling configuration consistency check

About disabling configuration consistency check

To ensure that the DR system can operate correctly, DRNI by default performs configuration consistency check when the DR system is set up.

Configuration consistency check might fail when you upgrade the DR member devices in a DR system. To prevent the DR system from falsely shutting down DR interfaces, you can temporarily disable configuration consistency check.

Configuration restrictions and guidelines

Make sure the DR member devices use the same setting for configuration consistency check.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable configuration consistency check.</td>
<td>drni consistency-check disable</td>
</tr>
</tbody>
</table>
Enabling the short DRCP timeout timer on the IPP or a DR interface

About the DRCP timeout timer
By default, the IPP or a DR interface uses the 90-second long DRCP timeout timer. To detect peer interface down events more quickly, enable the 3-second short DRCP timeout timer on the interface.

Configuration restrictions and guidelines
To avoid traffic interruption during an ISSU or DRNI process restart, disable the short DRCP timeout timer before you perform an ISSU or DRNI process restart. For more information about ISSU, see Fundamentals Configuration Guide.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view. | • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number  
• Enter VXLAN tunnel interface view: interface tunnel number | N/A |
| 3.   | Enable the short DRCP timeout timer. | drni drcp period short | By default, an aggregate interface uses the long DRCP timeout timer (90 seconds). |

Setting the keepalive hold timer for identifying the cause of IPL down events

About the keepalive hold timer
The keepalive hold timer starts when the IPL goes down. The keepalive hold timer specifies the amount of time that the device uses to identify the cause of an IPL down event.

- If the device receives keepalive packets from the DR peer before the timer expires, the IPL is down because the IPL fails.
- If the device does not receive keepalive packets from the DR peer before the timer expires, the IPL is down because the peer DR device fails.

Configuration restrictions and guidelines
For the DR member device to correctly determine the cause of an IPL down event, make sure the keepalive hold timer is longer than the keepalive interval and is shorter than the keepalive timeout timer.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the keepalive hold timer.</td>
<td>drni keepalive hold-time value</td>
</tr>
</tbody>
</table>
Configuring DR system auto-recovery

About DR system auto-recovery

If only one DR member device recovers after the entire DR system reboots, auto-recovery enables that member device to take over the primary role when the reload delay timer expires. Then, the member device can forward traffic through its DR interfaces.

If auto-recovery is disabled, that DR member device will be stuck in the None role with all its DR interfaces being down after it recovers.

Configuration restrictions and guidelines

This feature is supported in R2612 and later.

If both DR member devices recover after the entire DR system reboots, active-active situation might occur if both IPL and keepalive links were down when the reload delay timer expires. If this rare situation occurs, examine the IPL and keepalive links and restore them.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure DR system auto-recovery.</td>
<td>drni auto-recovery</td>
</tr>
</tbody>
</table>

Setting the data restoration interval

About the data restoration interval

The data restoration interval specifies the maximum amount of time for the secondary DR device to synchronize data with the primary DR device during DR system setup. Within the data restoration interval, the secondary DR device sets all network interfaces to DRNI MAD DOWN state, except for the interfaces excluded from the shutdown action by DRNI.

When the data restoration interval expires, the secondary DR device brings up all network interfaces.

Configuration restrictions and guidelines

Increase the data restoration interval as needed in the following situations:

- Avoid packet loss and forwarding failure that might occur when the amount of data is large or when you perform an ISSU between the DR member devices.
- Avoid DR interface flapping that might occur if type 1 configuration consistency check fails after the DR interfaces come up upon expiration of the data restoration interval.

Configuration procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the data restoration interval.</td>
<td>drni restore-delay</td>
</tr>
</tbody>
</table>
Displaying and maintaining DRNI

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the configuration consistency check done by DRNI.</td>
<td>`display drni consistency { type1</td>
</tr>
<tr>
<td>Display detailed DRNI MAD information.</td>
<td><code>display drni mad verbose</code></td>
</tr>
<tr>
<td>Display the DR system settings.</td>
<td><code>display drni system</code></td>
</tr>
<tr>
<td>Display brief information about the IPP and DR interfaces.</td>
<td><code>display drni summary</code></td>
</tr>
<tr>
<td>Display detailed information about the IPP and DR interfaces.</td>
<td><code>display drni verbose [ bridge-aggregation interface-number ]</code></td>
</tr>
<tr>
<td>Display DRCPDU statistics.</td>
<td><code>display drni drcp statistics [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Display DR keepalive packet statistics.</td>
<td><code>display drni keepalive</code></td>
</tr>
<tr>
<td>Display DR role information.</td>
<td><code>display drni role</code></td>
</tr>
<tr>
<td>Clear DRCPDU statistics.</td>
<td><code>reset drni drcp statistics [ interface interface-list ]</code></td>
</tr>
</tbody>
</table>

DRNI configuration examples

Basic DRNI configuration example

Network requirements

As shown in Figure 111, configure DRNI on Device A and Device B to establish a multichassis aggregate link with Device C.

Figure 111 Network diagram
Configuration procedure

1. Configure Device A:

   # Configure DR system settings.
   <DeviceA> system-view
   [DeviceA] drni system-mac 1-1-1
   [DeviceA] drni system-number 1
   [DeviceA] drni system-priority 123

   # Specify the source and destination IP addresses of the keepalive packets sent by the local DR member device.
   [DeviceA] drni keepalive ip destination 1.1.1.1 source 1.1.1.2

   # Configure Ten-GigabitEthernet 1/0/5 as a Layer 3 interface by setting its link mode to route mode. Assign the interface an IP address, which is the source IP address of keepalive packets.
   [DeviceA] interface ten-gigabitethernet 1/0/5
   [DeviceA-Ten-GigabitEthernet1/0/5] port link-mode route
   [DeviceA-Ten-GigabitEthernet1/0/5] ip address 1.1.1.2 24
   [DeviceA-Ten-GigabitEthernet1/0/5] quit

   # Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.
   Release 2609:
   [DeviceA] mad exclude interface ten-gigabitethernet 1/0/5
   R2612 and later:
   [DeviceA] drni mad exclude interface ten-gigabitethernet 1/0/5

   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.
   [DeviceA] interface bridge-aggregation 3
   [DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
   [DeviceA-Bridge-Aggregation3] quit

   # Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 3.
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 3
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
   [DeviceA-Ten-GigabitEthernet1/0/2] quit

   # Specify Bridge-Aggregation 3 as the IPP.
   [DeviceA] interface bridge-aggregation 3
   [DeviceA-Bridge-Aggregation3] port drni intra-portal-port 1
   [DeviceA-Bridge-Aggregation3] quit

   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.
   [DeviceA] interface bridge-aggregation 4
   [DeviceA-Bridge-Aggregation4] link-aggregation mode dynamic
   [DeviceA-Bridge-Aggregation4] quit

   # Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 4.
   [DeviceA] interface ten-gigabitethernet 1/0/3
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 4
   [DeviceA-Ten-GigabitEthernet1/0/3] quit
   [DeviceA] interface ten-gigabitethernet 1/0/4
   [DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 4
   [DeviceA-Ten-GigabitEthernet1/0/4] quit
# Assign Bridge-Aggregation 4 to DR group 4.
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] port drni group 4
[DeviceA-Bridge-Aggregation4] quit

2. Configure Device B:
# Configure DR system settings.
<DeviceB> system-view
[DeviceB] drni system-mac 1-1-1
[DeviceB] drni system-number 2
[DeviceB] drni system-priority 123
# Configure DR keepalive packet parameters.
[DeviceB] drni keepalive ip destination 1.1.1.2 source 1.1.1.1
# Set the link mode of Ten-GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port link-mode route
[DeviceB-Ten-GigabitEthernet1/0/5] ip address 1.1.1.1 24
[DeviceB-Ten-GigabitEthernet1/0/5] quit
# Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.
Release 2609:
[DeviceB] mad exclude interface ten-gigabitethernet 1/0/5
R2612 and later:
[DeviceB] drni mad exclude interface ten-gigabitethernet 1/0/5
# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] quit
# Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 3.
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceB-Ten-GigabitEthernet1/0/1] quit
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceB-Ten-GigabitEthernet1/0/2] quit
# Specify Bridge-Aggregation 3 as the IPP.
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation3] quit
# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation4] quit
# Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 4.
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port link-aggregation group 4
[DeviceB-Ten-GigabitEthernet1/0/3] quit
[DeviceB] interface ten-gigabitethernet 1/0/4
3. Configure Device C:

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 4
[DeviceC-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation4] quit

# Assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to aggregation group 4.
[DeviceC] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[DeviceC-if-range] port link-aggregation group 4
[DeviceC-if-range] quit

Verifying the configuration

# Verify that the keepalive link is working correctly on Device A.
[DeviceA] display drni keepalive
Neighbor keepalive link status: Up
Neighbor is alive for: 104 sec, 16 ms
Last keepalive packet sending status: Successful
Last keepalive packet sending time: 2017/03/09 10:12:09 620 ms
Last keepalive packet receiving status: Successful
Last keepalive packet receiving time: 2017/03/09 10:12:09 707 ms

Distributed relay keepalive parameters:
Destination IP address: 1.1.1.1
Source IP address: 1.1.1.2
Keepalive UDP port : 6400
Keepalive vpn-instance : N/A
Keepalive interval : 1000 ms
Keepalive timeout : 5 sec
Keepalive hold time: 3 sec
Keepalive UDP port : 6400

# Verify that the IPP and the DR interface are working correctly on Device A.
[DeviceA] display drni summary
Global consistency check : SUCCESS
Inconsistent type 1 global settings: -

IPP    IPP ID  State
BAGG3  1     UP

DR interface DR group ID State Check result Type 1 inconsistency
BAGG4  4     UP SUCCESS -

[DeviceA] display drni verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
G -- Port_Sync, H -- Expired

IPP/IPP ID: BAGG3/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports Index: 1, 2
Peer Selected ports Index: 1, 2

DR interface/DR group ID: BAGG4/4
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports Index: 16387, 16388
Peer Selected ports Index: 32771, 32772

# Verify that all member ports of aggregation group 4 are in Selected state on Device C, which indicates a successful link aggregation between the DR system and Device C.

```
[DeviceC] display link-aggregation verbose bridge-aggregation 4
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
Aggregate Interface: Bridge-Aggregation4
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANS: None
System ID: 0x8000, 2e56-cbae-0600
Local:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Priority Index</th>
<th>Oper-Key</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1(R)</td>
<td></td>
<td>32768</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td></td>
<td>32768</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td></td>
<td>32768</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>XGE1/0/4</td>
<td></td>
<td>32768</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote:

<table>
<thead>
<tr>
<th>Actor</th>
<th>Priority Index</th>
<th>Oper-Key SystemID</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/1</td>
<td>32768</td>
<td>16387</td>
<td>40004</td>
</tr>
<tr>
<td>XGE1/0/2</td>
<td>32768</td>
<td>16388</td>
<td>40004</td>
</tr>
<tr>
<td>XGE1/0/3</td>
<td>32768</td>
<td>32771</td>
<td>40004</td>
</tr>
<tr>
<td>XGE1/0/4</td>
<td>32768</td>
<td>32772</td>
<td>40004</td>
</tr>
</tbody>
</table>
```

**DRNI Layer 3 forwarding configuration example**

**Network requirements**

As shown in Figure 112:

- Configure Device A and Device B as a DR system to provide both link-level and node-level redundancy.
- Use Ten-GigabitEthernet 1/0/5 on Device A and Device B to establish the DR keepalive link.
Configure Device A and Device B to provide VRRP gateway services for VLAN 100 and VLAN 101 on VLAN-interface 100 at 10.1.1.100/24 and VLAN-interface at 20.1.1.100/24, respectively. Make sure Device A has higher priority than Device B in the VRRP groups to be elected as master.

**Figure 112 Network diagram**

**Configuration procedure**

1. Configure Device A:
   
   # Configure DR system settings.
   ```
   <DeviceA> system-view
   [DeviceA] drni system-mac 1-1-1
   [DeviceA] drni system-number 1
   [DeviceA] drni system-priority 123
   # Specify the source and destination IP addresses of the keepalive packets sent by the local DRNI member device.
   [DeviceA] drni keepalive ip destination 1.1.1.2 source 1.1.1.1
   # Configure Ten-GigabitEthernet 1/0/5 as a Layer 3 interface by setting its link mode to route mode. Assign the interface an IP address, which is the source IP address of keepalive packets.
   [DeviceA] interface ten-gigabitethernet 1/0/5
   [DeviceA-Ten-GigabitEthernet1/0/5] port link-mode route
   [DeviceA-Ten-GigabitEthernet1/0/5] ip address 1.1.1.2 24
   [DeviceA-Ten-GigabitEthernet1/0/5] quit
   # Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.
   Release 2609:
   [DeviceA] mad exclude interface ten-gigabitethernet 1/0/5
   R2612 and later:
   [DeviceA] drni mad exclude interface ten-gigabitethernet 1/0/5
   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 125 and specify it as the IPP.
   ```
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation125] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation125] quit

# Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 125.
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 125
[DeviceA-Ten-GigabitEthernet1/0/3] quit
[DeviceA] interface ten-gigabitethernet 1/0/4
[DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 125
[DeviceA-Ten-GigabitEthernet1/0/4] quit

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100 and assign it to DR group 1.
[DeviceA] interface bridge-aggregation 100
[DeviceA-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation100] port drni group 1
[DeviceA-Bridge-Aggregation100] quit

# Assign Ten-GigabitEthernet 1/0/1 to aggregation group 100.
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 100
[DeviceA-Ten-GigabitEthernet1/0/1] quit

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101 and assign it to DR group 2.
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation101] port drni group 2
[DeviceA-Bridge-Aggregation101] quit

# Assign Ten-GigabitEthernet 1/0/2 to aggregation group 101.
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceA-Ten-GigabitEthernet1/0/2] quit

# Create VLAN 100 and VLAN 101.
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 101
[DeviceA-vlan101] quit

# Configure Bridge-Aggregation 100 as a trunk port and assign it to VLAN 100.
[DeviceA] interface bridge-aggregation 100
[DeviceA-Bridge-Aggregation100] port link-type trunk
[DeviceA-Bridge-Aggregation100] port trunk permit vlan 100
[DeviceA-Bridge-Aggregation100] quit

# Configure Bridge-Aggregation 101 as a trunk port and assign it to VLAN 101.
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] port link-type trunk
[DeviceA-Bridge-Aggregation101] port trunk permit vlan 101
[DeviceA-Bridge-Aggregation101] quit

# Configure Bridge-Aggregation 125 as a trunk port and assign it to VLAN 100 and VLAN 101.
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] port link-type trunk
[DeviceA-Bridge-Aggregation125] port trunk permit vlan 100 101
[DeviceA-Bridge-Aggregation125] quit

# Create VLAN-interface 100 and VLAN-interface 101, and assign IP addresses to them.
[DeviceA] interface vlan-interface 100
[DeviceA-vlan-interface100] ip address 10.1.1.1 24
[DeviceA-vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-vlan-interface101] ip address 20.1.1.1 24
[DeviceA-vlan-interface101] quit

# Configure OSPF.
[DeviceA] ospf
[DeviceA-ospf-1] import-route direct
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceA-ospf-1] quit

# Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 10.1.1.100.
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 virtual-ip 10.1.1.100

# Assign a priority of 200 to Device A in VRRP group 1.
[DeviceA-Vlan-interface100] vrrp vrid 1 priority 200
[DeviceA-Vlan-interface100] quit

# Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 20.1.1.100.
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 2 virtual-ip 20.1.1.100

# Assign a priority of 200 to Device A in VRRP group 2.
[DeviceA-Vlan-interface101] vrrp vrid 2 priority 200
[DeviceA-Vlan-interface100] quit

2. Configure Device B:

# Configure DR system settings:
<DeviceB> system-view
[DeviceB] drni system-mac 1-1-1
[DeviceB] drni system-number 2
[DeviceB] drni system-priority 123

# Specify the source and destination IP addresses of the keepalive packets sent by the local DRNI member device.
[DeviceB] drni keepalive ip destination 1.1.1.1 source 1.1.1.2

# Configure Ten-GigabitEthernet 1/0/5 as a Layer 3 interface by setting its link mode to route mode. Assign the interface an IP address, which is the source IP address of keepalive packets.
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port link-mode route
[DeviceB-Ten-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceB-Ten-GigabitEthernet1/0/5] quit

# Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.
Release 2609:
# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 125 and specify it as the IPP.

```
DeviceB interface bridge-aggregation 125
DeviceB-Bridge-Aggregation125 link-aggregation mode dynamic
DeviceB-Bridge-Aggregation125 port drni intra-portal-port 1
DeviceB-Bridge-Aggregation125 quit
```

# Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 125.

```
DeviceB interface ten-gigabitethernet1/0/3
DeviceB-Ten-GigabitEthernet1/0/3 port link-aggregation group 125
DeviceB-Ten-GigabitEthernet1/0/3 quit

DeviceB interface ten-gigabitethernet 1/0/4
DeviceB-Ten-GigabitEthernet1/0/4 port link-aggregation group 125
DeviceB-Ten-GigabitEthernet1/0/4 quit
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100 and assign it to DR group 1.

```
DeviceB interface bridge-aggregation 100
DeviceB-Bridge-Aggregation100 link-aggregation mode dynamic
DeviceB-Bridge-Aggregation100 port drni group 1
DeviceB-Bridge-Aggregation100 quit
```

# Assign Ten-GigabitEthernet 1/0/1 to aggregation group 100.

```
DeviceB interface ten-gigabitethernet 1/0/1
DeviceB-Ten-GigabitEthernet1/0/1 port link-aggregation group 100
DeviceB-Ten-GigabitEthernet1/0/1 quit
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101 and assign it to DR group 2.

```
DeviceB interface bridge-aggregation 101
DeviceB-Bridge-Aggregation101 link-aggregation mode dynamic
DeviceB-Bridge-Aggregation101 port drni group 2
DeviceB-Bridge-Aggregation101 quit
```

# Assign Ten-GigabitEthernet 1/0/2 to aggregation group 101.

```
DeviceB interface ten-gigabitethernet 1/0/2
DeviceB-Ten-GigabitEthernet1/0/2 port link-aggregation group 101
DeviceB-Ten-GigabitEthernet1/0/2 quit
```

# Create VLAN 100 and VLAN 101.

```
DeviceB vlan 100
DeviceB-vlan100 quit

DeviceB vlan 101
DeviceB-vlan101 quit
```

# Configure Bridge-Aggregation 100 as a trunk port and assign it to VLAN 100.

```
DeviceB interface bridge-aggregation 100
DeviceB-Bridge-Aggregation100 port link-type trunk
DeviceB-Bridge-Aggregation100 port trunk permit vlan 100
DeviceB-Bridge-Aggregation100 quit
```

# Configure Bridge-Aggregation 101 as a trunk port and assign it to VLAN 101.

```
DeviceB interface bridge-aggregation 101
```
# Configure Bridge-Aggregation 101 as a trunk port and assign it to VLAN 101.

[DeviceB-Bridge-Aggregation101] port link-type trunk

[DeviceB-Bridge-Aggregation101] port trunk permit vlan 101

[DeviceB-Bridge-Aggregation101] quit

# Configure Bridge-Aggregation 125 as a trunk port and assign it to VLAN 100 and VLAN 101.

[DeviceB] interface bridge-aggregation 125

[DeviceB-Bridge-Aggregation125] port link-type trunk

[DeviceB-Bridge-Aggregation125] port trunk permit vlan 100 101

[DeviceB-Bridge-Aggregation125] quit

# Create VLAN-interface 100 and VLAN-interface 101, and assign IP addresses to them.

[DeviceB] interface vlan-interface 100

[DeviceB-vlan-interface100] ip address 10.1.1.2 24

[DeviceB-vlan-interface100] quit

[DeviceB] interface vlan-interface 101

[DeviceB-vlan-interface101] ip address 20.1.1.2 24

[DeviceB-vlan-interface101] quit

# Configure OSPF.

[DeviceB] ospf

[DeviceB-ospf-1] import-route direct

[DeviceB-ospf-1] area 0

[DeviceB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255

[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255

[DeviceB-ospf-1-area-0.0.0.0] quit

[DeviceB-ospf-1] quit

# Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 10.1.1.100.

[DeviceB] interface vlan-interface 100

[DeviceB-Vlan-interface100] vrrp vrid 1 virtual-ip 10.1.1.100

[DeviceB-Vlan-interface100] quit

# Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 20.1.1.100.

[DeviceB] interface vlan-interface 101

[DeviceB-Vlan-interface101] vrrp vrid 2 virtual-ip 20.1.1.100

[DeviceB-Vlan-interface101] quit

3. Configure Device C:

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100.

<DeviceC> system-view

[DeviceC] interface bridge-aggregation 100

[DeviceC-Bridge-Aggregation100] link-aggregation mode dynamic

[DeviceC-Bridge-Aggregation100] quit

# Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 100.

[DeviceC] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/2

[DeviceC-if-range] port link-aggregation group 100

[DeviceC-if-range] quit

# Create VLAN 100.

[DeviceC] vlan 100

[DeviceC-vlan100] quit

# Configure Bridge-Aggregation 100 as a trunk port and assign it to VLAN 100.

[DeviceC] interface bridge-aggregation 100

[DeviceC-Bridge-Aggregation100] port link-type trunk
4. Configure Device D:

   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101.
   <DeviceD> system-view
   [DeviceD] interface bridge-aggregation 101
   [DeviceD-Bridge-Aggregation101] link-aggregation mode dynamic
   [DeviceD-Bridge-Aggregation101] quit

   # Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 101.
   [DeviceD] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/2
   [DeviceD-if-range] port link-aggregation group 101
   [DeviceD-if-range] quit

   # Create VLAN 101.
   [DeviceD] vlan 101
   [DeviceD-vlan101] quit

   # Configure Bridge-Aggregation 101 as a trunk port and assign it to VLAN 100.
   [DeviceD] interface bridge-aggregation 101
   [DeviceD-Bridge-Aggregation101] port link-type trunk
   [DeviceD-Bridge-Aggregation101] port trunk permit vlan 101
   [DeviceD-Bridge-Aggregation101] quit

   # Configure Ten-GigabitEthernet 1/0/3 as a trunk port and assign it to VLAN 101.
   [DeviceD] interface ten-gigabitethernet 1/0/3
   [DeviceD-Ten-GigabitEthernet1/0/3] port link-type trunk
   [DeviceD-Ten-GigabitEthernet1/0/3] port trunk permit vlan 101
   [DeviceD-Ten-GigabitEthernet1/0/3] quit

   # Create VLAN-interface 101 and assign an IP address to it.
   [DeviceD] interface vlan-interface 101
   [DeviceD-vlan-interface101] ip address 20.1.1.3 24
   [DeviceD-vlan-interface101] quit

   # Configure OSPF.
   [DeviceD] ospf
   [DeviceD-ospf-1] import-route direct
   [DeviceD-ospf-1] area 0
   [DeviceD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
   [DeviceD-ospf-1-area-0.0.0.0] quit
   [DeviceD-ospf-1] quit
Verifying the configuration

# Verify that Device C has established OSPF neighbor relationships with Device A and Device B correctly.
[DeviceC] display ospf peer

OSPF Process 1 with Router ID 10.1.1.3
Neighbor Brief Information

Area: 0.0.0.0
Router ID   Address   Pri Dead-Time State   Interface
20.1.1.1    10.1.1.1   1   37 Full/DR   Vlan100
20.1.1.2    10.1.1.2   1   32 Full/BDR   Vlan100

# Verify that Device D has established OSPF neighbor relationships with Device A and Device B correctly.
[DeviceD] display ospf peer

OSPF Process 1 with Router ID 20.1.1.3
Neighbor Brief Information

Area: 0.0.0.0
Router ID   Address   Pri Dead-Time State   Interface
20.1.1.1    20.1.1.1   1   38 Full/DR   Vlan101
20.1.1.2    20.1.1.2   1   37 Full/BDR   Vlan101

# Verify that Host A and Host B can ping each other. (Details not shown.)
Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

**Command conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td><em>Italic</em> text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>&amp;&lt;1-n&gt;</td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

**GUI conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in Boldface. For example, the <em>New User</em> window opens; click OK.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, File &gt; Create &gt; Folder.</td>
</tr>
</tbody>
</table>

**Symbols**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>△ WARNING!</td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>△ CAUTION:</td>
<td>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.</td>
</tr>
<tr>
<td>☰ IMPORTANT:</td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>✡ TIP:</td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
# Network topology icons

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Generic Device" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="image2" alt="Routing Device" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="image3" alt="Layer 2/3 Switch" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="image4" alt="Access Controller" /></td>
<td>Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.</td>
</tr>
<tr>
<td><img src="image5" alt="Access Point" /></td>
<td>Represents an access point.</td>
</tr>
<tr>
<td><img src="image6" alt="Wireless Terminator Unit" /></td>
<td>Represents a wireless terminator unit.</td>
</tr>
<tr>
<td><img src="image7" alt="Wireless Terminator" /></td>
<td>Represents a wireless terminator.</td>
</tr>
<tr>
<td><img src="image8" alt="Mesh Access Point" /></td>
<td>Represents a mesh access point.</td>
</tr>
<tr>
<td><img src="image9" alt="Omnidirectional Signals" /></td>
<td>Represents omnidirectional signals.</td>
</tr>
<tr>
<td><img src="image10" alt="Directional Signals" /></td>
<td>Represents directional signals.</td>
</tr>
<tr>
<td><img src="image11" alt="Security Product" /></td>
<td>Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.</td>
</tr>
<tr>
<td><img src="image12" alt="Security Module" /></td>
<td>Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.</td>
</tr>
</tbody>
</table>

**Examples provided in this document**

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website: http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website: http://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: http://www.hpe.com/support/e-updates
  - Software Depot website: http://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: http://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

<table>
<thead>
<tr>
<th>Website</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Networking websites</strong></td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library for Networking</td>
<td><a href="http://www.hpe.com/networking/resourcefinder">http://www.hpe.com/networking/resourcefinder</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking website</td>
<td><a href="http://www.hpe.com/info/networking">http://www.hpe.com/info/networking</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise My Networking website</td>
<td><a href="http://www.hpe.com/networking/support">http://www.hpe.com/networking/support</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking Warranty</td>
<td><a href="http://www.hpe.com/networking/warranty">http://www.hpe.com/networking/warranty</a></td>
</tr>
<tr>
<td><strong>General websites</strong></td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library</td>
<td><a href="http://www.hpe.com/info/enterprise/docs">http://www.hpe.com/info/enterprise/docs</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Center</td>
<td><a href="http://www.hpe.com/support/hpesc">http://www.hpe.com/support/hpesc</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Services Central</td>
<td><a href="http://ssc.hpe.com/portal/site/ssc/">http://ssc.hpe.com/portal/site/ssc/</a></td>
</tr>
<tr>
<td>Contact Hewlett Packard Enterprise Worldwide</td>
<td><a href="http://www.hpe.com/assistance">http://www.hpe.com/assistance</a></td>
</tr>
<tr>
<td>Subscription Service/Support Alerts</td>
<td><a href="http://www.hpe.com/support/e-updates">http://www.hpe.com/support/e-updates</a></td>
</tr>
<tr>
<td>Software Depot</td>
<td><a href="http://www.hpe.com/support/softwaredepot">http://www.hpe.com/support/softwaredepot</a></td>
</tr>
<tr>
<td>Customer Self Repair (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/support/selfrepair">http://www.hpe.com/support/selfrepair</a></td>
</tr>
<tr>
<td>Insight Remote Support (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/info/insightremotesupport/docs">http://www.hpe.com/info/insightremotesupport/docs</a></td>
</tr>
</tbody>
</table>

**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:

http://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:

http://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 (mailto: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
0:2 VLAN mapping
  application scenario, 255
  implementation, 257
1:1 VLAN mapping
  application scenario, 255, 255
  configuration, 261, 267
  implementation, 257, 258
1:2 VLAN mapping
  application scenario, 255, 256
  configuration, 266, 273
  implementation, 257, 259
10-GE interface; 0:10-GE interface combine, 2
2:2 VLAN mapping
  application scenario, 255, 256
  configuration, 267, 273
  implementation, 257, 259
2:3 VLAN mapping
  application scenario, 255
  implementation, 257
40-GE interface; 0:40-GE interface split, 2
802
  802.1 LLDPDU TLV types, 288
  802.1ah PBB configuration, 276
  802.1Q-in-802.1Q. Use QinQ
  802.3 LLDPDU TLV types, 288
  LLDP 802.1p-to-local priority mapping, 307
  LLDP PFC 802.1p priority, 309
  QinQ SVLAN tag 802.1p priority, 249
802.1X
  VLAN group configuration, 182
A
accessing
  port-based VLAN assignment (access port), 173
ACL
  LLDP APP parameter, 305
  LLDP DCBX version, 305
action
  loop detection block, 161
  loop detection no-learning protection, 161
  loop detection protection action (Layer 2 aggregate interface), 163
  loop detection protection action (S-channel aggregate interface), 163
  loop detection protection action (S-channel bundle interface), 163
  loop detection protection action setting, 163
  loop detection shutdown protection, 161
adding
  MAC address table blackhole entry, 30
  MAC address table entry (global), 29
  MAC address table entry (on interface), 30
  MAC address table multiport unicast entry, 31
address
  Ethernet interface MAC address (Layer 3), 20
  Ethernet subinterface MAC address (Layer 3), 20
  MAC address learning disable, 32
  MAC address table learning limit, 34
  MAC Information queue length, 43
advertising
  LLDP advertisable TLV, 295
  LLDP+DCBX TLV advertisement, 304
  voice VLAN advertisement (CDP), 222
  voice VLAN advertisement (LLDP), 222
  voice VLAN information advertisement to IP phones, 214
aggregating
  link. See link aggregation
aging
  MAC address table timer, 33
  spanning tree max age timer, 125
algorithm
  Ethernet link aggregation load sharing algorithm settings, 72
  STP calculation, 100
alternate port (MST), 113
APP parameter (LLDP), 305
ARP
  LLDP ARP entry generation, 311
  MAC address table ARP fast update, 38
ARP detection
  M:1 VLAN mapping (dynamic IP address assignment), 262
ARP snooping
  M:1 VLAN mapping (static IP address assignment), 264
assigning
  aggregate interface to DR group, 346
  MAC address table learning priority, 34
MAC-based VLAN assignment (dynamic), 176
MAC-based VLAN assignment (server-assigned), 177
MAC-based VLAN assignment (static), 175
port isolation group (multiple ports), 94
port-based VLAN access port, 173
port-based VLAN access port (interface view), 173
port-based VLAN access port (VLAN view), 173
port-based VLAN hybrid port, 174
port-based VLAN trunk port, 173
voice VLAN assignment mode (automatic), 215
voice VLAN assignment mode (manual), 216
attachment circuit (AC)
  PBB, 277
attribute
  Ethernet link aggregation attribute configuration, 47
auto
  loop detection port status auto recovery, 161
voice VLAN assignment (automatic), 215
voice VLAN assignment mode configuration (automatic), 223
voice VLAN LLDP automatic IP phone discovery enable, 221
voice VLAN port operation configuration (automatic assignment), 219
AutoMDIX mode (Ethernet interface), 18
B
backbone
  core bridge. See BCB
edge bridge. See BEB
MAC address. See B-MAC
PBB configuration, 276, 280, 283
PBB core bridge network model, 276
PBB edge bridge network model, 276
service instance identifier. See I-SID
VLAN. See B-VLAN
backing up
  MST backup port, 113
bandwidth
  Ethernet link aggregate interface (expected bandwidth), 65
  LLDP ETS parameters, 307
basic management LLDPDU TLV types, 288
BFD
  Ethernet link aggregation group BFD, 66
blackhole
  MAC address table, 27
MAC address table entry, 30
block action (loop detection), 161
boundary port (MST), 113
BPDU
  configuration BPDU, 97
  MST region max hops, 124
  MSTP BPDU protocol frames, 109
  PVST BPDU guard, 146
  RSTP BPDU processing, 107
  spanning tree BPDU drop, 145
  spanning tree BPDU guard, 142
  spanning tree BPDU transparent transmission (on port), 148
  spanning tree hello time, 125
  spanning tree max age timer, 125
  spanning tree TC BPDU event logging (PVST mode), 148
  spanning tree TC-BPDU guard, 145
  spanning tree TC-BPDU transmission restriction, 144
  STP BPDU forwarding, 105
TCN BPDU, 98
transmission rate configuration, 127
bridging
  Ethernet interface bridging enable (Layer 2), 19
  LLDP agent customer bridge, 286
  LLDP agent nearest bridge, 286
  LLDP agent non-TPMR bridge, 286
  LLDP bridge mode configuration, 293
  MST common root bridge, 113
  MST regional root, 112
  PBB network model, 276
  spanning tree dispute guard, 146
  spanning tree loop guard, 143
  spanning tree root bridge, 123
  spanning tree root bridge (device), 123
  spanning tree root guard, 143
  spanning tree secondary root bridge (device), 124
  STP designated bridge, 99
  STP root bridge, 99
bulk
  interface configuration, 25, 25
  interface configuration display, 26
  interface configuration restrictions, 25
B-VLAN
  PBB VSI configuration, 281
C
  cable
    Ethernet interface cable connection (Layer 2), 19
  calculating
MSTI calculation, 114
MSTP CIST calculation, 114
spanning tree port path cost calculation standard, 128
spanning tree timeout factor, 127
STP algorithm, 100
CDP
LLDP CDP compatibility, 301
LLDP CDP-compatible configuration, 316
voice VLAN advertisement, 222
voice VLAN information advertisement to IP phones, 214
CE
L2PT configuration, 323, 325, 327
L2PT for LACP configuration, 328
L2PT for STP configuration, 327
changing
Ethernet aggregate interface (MAC address), 62
Ethernet interface to FC interface (Layer 2), 16
checking
spanning tree No Agreement Check, 138, 140
choosing
Ethernet link aggregation reference port, 48, 52
Cisco
Discovery Protocol. Use CDP
LLDP CDP compatibility, 301
LLDP configuration (CDP-compatible), 316
CIST
calculation, 114
network device connection, 112
spanning tree max age timer, 125
combining
Ethernet interfaces (10-GE > 40-GE), 2
common root bridge, 113
configuring
1:1 VLAN mapping, 261, 267
1:2 VLAN mapping, 266, 273
2:2 VLAN mapping, 267, 273
common Ethernet interface settings, 2
DR keepalive packet parameters, 345
DR keepalive settings, 344
DR system MAC, 342
DR system number, 342
DR system priority, 343
DR system settings, 342
DRNI with PVST, 157
Ethernet aggregate interface, 61
Ethernet aggregate interface (description), 61
Ethernet interface, 1
Ethernet interface (Layer 2), 15
Ethernet interface (Layer 3), 20
Ethernet interface basic settings, 4
Ethernet interface dampening, 7
Ethernet interface generic flow control, 10
Ethernet interface jumbo frame support, 6
Ethernet interface link mode, 5
Ethernet interface PFC, 11
Ethernet interface physical state change suppression, 6
Ethernet interface storm control (Layer 2), 15
Ethernet interface storm suppression, 14
Ethernet link aggregate interface (Layer 2 edge), 85
Ethernet link aggregation, 46, 55, 79
Ethernet link aggregation (Layer 2 dynamic), 80
Ethernet link aggregation (Layer 2 static), 79
Ethernet link aggregation (Layer 3 dynamic), 87
Ethernet link aggregation (Layer 3 static), 86
Ethernet link aggregation edge aggregate interface, 65
Ethernet link aggregation group, 56
Ethernet link aggregation group (Layer 2 dynamic), 57
Ethernet link aggregation group (Layer 2 static), 57
Ethernet link aggregation group (Layer 3 dynamic), 59
Ethernet link aggregation group (Layer 3 static), 58
Ethernet link aggregation group BFD, 66
Ethernet link aggregation group load sharing, 69
Ethernet link aggregation load sharing (Layer 2), 82
Ethernet link aggregation load sharing (Layer 3), 89
Ethernet subinterface (Layer 3), 20
Ethernet subinterface basic settings, 4
interface (inloopback), 24
interface (loopback), 23
interface (null), 23
interfaces in bulk, 25, 25
IP subnet-based VLAN, 180, 187
L2PT, 323, 325, 327
L2PT for LACP, 328
L2PT for STP, 327
Layer 2 forwarding (cut-through), 334
LLDP, 286, 292, 312
LLDP (CDP-compatible), 316
LLDP 802.1p-to-local priority mapping, 307
LLDP advertisable TLVs, 295
VLAN interface, 170
VLAN mapping, 255, 260, 267
voice VLAN, 213, 218, 223
voice VLAN advertisement (CDP), 222
voice VLAN advertisement (LLDP), 222
voice VLAN assignment mode (automatic), 223
voice VLAN assignment mode (manual), 225
voice VLAN port operation (automatic assignment), 219
voice VLAN port operation (manual assignment), 220
voice VLAN traffic QoS priority settings, 218

connecting
Ethernet interface cable connection (Layer 2), 19
voice VLAN host+IP phone connection (in series), 214
voice VLAN IP phone+device, 215

Converged Enhanced Ethernet. Use CEE

CoS
voice VLAN traffic QoS priority settings, 218

cost
spanning tree port path cost calculation standard, 128
spanning tree port path cost configuration, 128, 131
STP path cost, 100

creating
PBB VSI, 280
super VLAN sub-VLAN, 192

CST
MST region connection, 112
customer
LLDP customer bridge mode, 293
cut-through Layer 2 forwarding configuration, 334

CVLAN
QinQ basic configuration, 251
QinQ configuration, 245, 251
QinQ VLAN transparent transmission configuration, 253
VLAN mapping application scenario, 255
VLAN mapping configuration, 255, 260, 267
VLAN mapping implementation, 257

D
dampening
Ethernet interface dampening, 7
data
PBB data encapsulation type, 282

Data Center
Bridging Exchange Protocol. Use DCBX

DCBX
configuration, 303, 317
LLDP APP parameter configuration, 305
LLDP DCBX version configuration, 305
LLDP ETS parameter configuration, 307
LLDP PFC parameter configuration, 309
LLDP+DCBX TLV advertisement, 304

DCBX version (LLDP), 305
default
Ethernet link aggregate interface default settings, 69
designated
MST port, 113
STP bridge, 99
STP port, 99
detecting
Ethernet link aggregation group BFD, 66
device
disabling the device to reactivate the shutdown edge ports, 148
Ethernet interface configuration, 1
Layer 2 forwarding configuration (cut-through), 334
LLDP basic configuration, 293, 312
LLDP CDP compatibility, 301
LLDP configuration, 286, 292, 312
LLDP configuration (CDP-compatible), 316
LLDP DCBX configuration, 303, 317, 317
LLDP parameters, 299
loop protection actions, 161
MSTP implementation, 115
MVRP configuration, 228, 231, 234
PVST BPDU guard, 146
spanning tree BPDU drop, 145
spanning tree BPDU guard, 142
spanning tree Digest Snooping, 136, 137
spanning tree dispute guard, 146
spanning tree inconsistent PVID protection disable, 136
spanning tree loop guard, 143
spanning tree No Agreement Check, 138, 140
spanning tree port role restriction, 144
spanning tree priority, 124
spanning tree protection, 142
spanning tree root guard, 143
spanning tree SNMP notification (new-root election, topology change events), 149
spanning tree TC BPDU event logging (PVST mode), 148
spanning tree TC Snooping, 140
spanning tree TC-BPDU guard, 145
spanning tree TC-BPDU transmission restriction, 144
voice VLAN IP phone+device connection, 215

DHCP snooping
  M:1 VLAN mapping, 262
diameter
  spanning tree switched network diameter, 125
Digest Snoop (spanning tree), 136, 137
directing
  Ethernet link aggregation traffic redirection, 72
disabling
  LLDP PVID inconsistency check, 300
  MAC address learning (global), 32
  MAC address learning (on interface), 32
  MAC address learning (on VLAN), 33
  MAC address table static source check, 38
  spanning tree dispute guard, 146
  spanning tree inconsistent PVID protection, 136
discarding
  MST discarding port state, 114
displaying
  bulk interface configuration, 26
  DRNI, 350
  Ethernet interface, 21
  Ethernet link aggregation, 78
  Ethernet subinterface, 21
  interface, 24
  L2PT, 326
  LLDP, 311
  loop detection, 164
  MAC address table, 40
  MVRP, 234
  PBB, 283
  port isolation, 94
  private VLAN, 200
  QinQ, 250
  service loopback group, 333
  spanning tree, 149
  super VLAN, 193
  VLAN, 183
  VLAN mapping, 267
  voice VLAN, 223
dispute
  spanning tree dispute guard, 146
distance
  Ethernet interface connection distance (Layer 2), 20
distributed relay
  DR group, 335
  DR group configuration, 346
  DR interface, 335
  DR interface assignment, 346
  DR keepalive settings, 344
  DR member device role, 336
  DR system MAC, 342
  DR system number, 342
  DR system priority, 343
  DR system settings, 342
  IPP specification, 347

Dot1
  spanning tree dot1d-1998 (port path cost calculation), 128
  spanning tree dot1t (port path cost calculation), 128
  dot1s (STP port mode), 133
downlink
  PBB port configuration, 281
DR interface
  DR interface assignment, 346
  failure handling mechanism, 339
  short DRCP timeout timer, 348
DR member device
  configuration consistency check, 338
  disabling configuration consistency check, 347
  DR keepalive settings, 344
  DR system MAC configuration, 342
  DR system number configuration, 342
  DR system priority configuration, 343
  DR system settings, 342
  DR system setup, 337
  failure handling mechanism, 339
  MAD mechanism, 337
DR system auto-recovery
  DRNI reload delay timer, 349
DRCP
  DR member device role, 336
  DR role priority, 336
  short DRCP timeout timer, 348
  timeout timers, 336, 336
DRNI
  configuration, 335, 350
  configuration consistency check, 338
  configuration restrictions, 341
  disabling configuration consistency check, 347
display, 350
  Distributed Relay Control Protocol, 336
  DR group, 335, 346
  DR group configuration, 350
  DR interface, 335, 346
  DR system setup, 337
failover mechanism, 336
failure handling, 339
failure handling mechanism, 339
intra-portal link (IPL), 335
intra-portal port (IPP), 335
IPP specification, 347
keepalive mechanism, 336
MAD mechanism, 337
maintain, 350
network model, 335
protocols and standards, 341
DRNI with PVST
configuration, 157
DSCP
voice VLAN traffic QoS priority settings, 218
dynamic
Ethernet link aggregation (Layer 2), 80
Ethernet link aggregation (Layer 3), 87
Ethernet link aggregation edge aggregate interface, 54
Ethernet link aggregation group, 57, 58
Ethernet link aggregation group BFD, 66
Ethernet link aggregation mode, 48
Layer 2 Ethernet link aggregation group, 57
Layer 3 Ethernet link aggregation group, 59
MAC address table dynamic aging timer, 33
MAC address table entry, 27
MAC address table entry configuration (global), 29
MAC address table entry configuration (on interface), 30
MAC-based VLAN assignment, 176, 178
S-channel bundle group, 60
S-MLAG (Layer 2), 91

E
edge
Ethernet link aggregate interface (Layer 2 edge), 85
STP edge port rapid transition, 115
dynamic
edge port
MST, 113
spanning tree, 128
enabling
Ethernet interface bridging (Layer 2), 19
Ethernet interface link flapping protection, 8
Ethernet interface loopback testing, 9
Ethernet link aggregation traffic redirection, 72
Ethernet subinterface packet statistics, 21
L2PT, 325
L2PT (for protocol), 325
Layer 3 aggregate subinterface packet statistics, 68
LLDP, 293
LLDP ARP entry generation, 311
LLDP polling, 295
LLDP+DCBX TLV advertisement, 304
loop detection (global), 162
loop detection (port-specific), 162
M:1 VLAN mapping ARP detection (dynamic IP address assignment), 262
M:1 VLAN mapping ARP snooping (static IP address assignment), 264
M:1 VLAN mapping DHCP snooping (dynamic IP address assignment), 262
MAC address synchronization, 35
MAC address table ARP fast update, 38
MAC address table move notification, 37
MAC address table SNMP notification, 39
MAC Information, 42
MVRP, 232
MVRP GVRP compatibility, 234
PBB L2VPN, 280
port bridging on Layer 2 aggregate interface, 75
PVST BPDU guard, 146
QinQ, 247
remote fault signal detection, 15
short DRCP timeout timer, 348
spanning tree BPDU drop, 145
spanning tree BPDU guard (global), 142
spanning tree BPDU guard (on interface), 142
spanning tree BPDU transparent transmission (on port), 148
spanning tree feature, 134
spanning tree loop guard, 143
spanning tree port state transition information output, 133
spanning tree root guard, 143
spanning tree SNMP notification (new-root election, topology change events), 149
spanning tree TC BPDU event logging (PVST mode), 148
spanning tree TC-BPDU guard, 145
transparent LACPDU transmission on VPLS network, 76
voice VLAN LLDP automatic IP phone discovery, 221
encapsulating
L2PT configuration, 323, 325, 327
L2PT for LACP configuration, 328
L2PT for STP configuration, 327
LLDP frame encapsulation (Ethernet II), 287
LLDP frame encapsulation (SNAP), 287
LLDP frame encapsulation format, 300
PBB data encapsulation type, 282
VLAN frame encapsulation, 168

Ethernet
ARP entry generation, 311
interface. See Ethernet interface
link aggregation. See Ethernet link aggregation
LLDP APP parameters, 305
LLDP DCBX configuration, 303, 317
LLDP DCBX version, 305
LLDP ETS parameters, 307
LLDP frame encapsulation, 287
LLDP group-based WRR queuing, 308
LLDP PFC parameters, 309
LLDP trapping, 309
LLDP+DCBX TLV advertisement, 304
LLDP-MED trapping, 309
loop detection configuration, 160, 164
loop detection protection action (Layer 2 Ethernet interface), 163
MAC address table configuration, 27, 28, 40
MAC Information configuration, 42, 43
PBB data encapsulation type, 282
port isolation configuration, 94
port isolation configuration (multiple isolation groups), 95
port-based VLAN assignment (access port), 173
port-based VLAN assignment (hybrid port), 174
port-based VLAN assignment (trunk port), 173
port-based VLAN configuration, 171
private VLAN configuration, 197, 198, 200
private VLAN promiscuous port configuration, 200
private VLAN trunk promiscuous port configuration, 203
private VLAN trunk promiscuous+secondary port configuration, 206
QinQ CVLAN frame header tag, 245
QinQ SVLAN frame header tag, 245
secondary VLAN Layer 3 communication configuration, 210
service loopback group configuration, 332, 333
subinterface. See Ethernet interface, Ethernet subinterface, subinterface
subinterface packet statistics, 21
super VLAN configuration, 192, 192, 194
super VLAN sub-VLAN creation, 192
VLAN basic configuration, 169
VLAN configuration, 168, 183
VLAN frame encapsulation, 168
VLAN interface, 170
VLAN port-based configuration, 183
voice VLAN configuration, 213, 218, 223

Ethernet interface
10-GE > 40-GE combine;010-GE > 40-GE combine, 2
40-GE split;040-GE split, 2
basic settings configuration, 4
bridging enable (Layer 2), 19
cable connection (Layer 2), 19
change to FC interface (Layer 2), 16
common settings configuration, 2
configuration, 1
configuration (Layer 2), 15
configuration (Layer 3), 20
distance (Layer 2), 20
dampening, 7
dampening restrictions, 8
display, 21
fiber port (Layer 2), 17
fiber port restrictions (Layer 2), 18
generic flow control, 10
jumbo frame support configuration, 6
link flapping protection, 8
link flapping protection restrictions, 9
link mode, 5
loopback test restrictions, 9
loopback testing, 9
MAC address (Layer 3), 20
maintain, 21
management interface configuration, 1
MDIX mode (Layer 2), 18
MTU setting (Layer 3), 20
naming conventions, 1
PFC configuration, 11
PFC configuration restrictions, 11
PFC thresholds, 12
physical state change suppression, 6
remote fault signal detection, 15
statistics polling interval, 13
storm control (Layer 2), 15
storm control configuration restrictions (Layer 2), 16
storm suppression, 14
storm suppression restrictions, 14

Ethernet link aggregation
aggregate group Selected ports min/max, 64
aggregate interface, 46
aggregate interface (description), 61
aggregate interface (MAC address), 62
aggregate interface configuration, 61
aggregate interface default settings, 69
aggregate interface shutdown, 68
aggregate interface types, 46
aggregation group, 46
aggregation group restrictions, 56
BFD configuration, 66
BFD configuration restrictions, 66
configuration, 46, 55, 79
configuration types, 47
default link-aggregation load sharing ignored packet fields, 70
display, 78
dynamic link aggregation, 50
dynamic link aggregation mode, 48
edge aggregate interface, 54, 65
group (Layer 3 dynamic), 59
group (Layer 3 static), 58
group configuration, 56
group configuration (Layer 2), 57
group configuration (Layer 3), 58
group load sharing configuration, 69
group load sharing mode, 69
how dynamic link aggregation works, 52
interface configuration (expected bandwidth), 65
LACP, 50
Layer 2 aggregate interface (ignored VLAN), 62, 62
Layer 2 aggregate interface (Layer 2 edge), 85
Layer 2 aggregate configuration (dynamic), 80
Layer 2 aggregate configuration (S-MLAG), 91
Layer 2 aggregate configuration (static), 79
Layer 2 aggregate load sharing (Layer 2), 82
Layer 2 group (dynamic), 57
Layer 2 group (static), 57
Layer 3 aggregate interface configuration (MTU), 63
Layer 3 aggregate subinterface packet statistics, 68
Layer 3 aggregation configuration (dynamic), 87
Layer 3 aggregation configuration (static), 86
Layer 3 aggregation configuration load sharing, 89
load sharing algorithm settings, 72
load sharing mode, 54
load sharing state, 47
local-first load sharing, 71
maintain, 78
management subnet, 74
management VLAN+management port, 74
member port, 46
member port state, 47, 49, 53
member port state (port speed), 63
modes, 48
operational key, 47
port speed in reference port selection, 67
reference port, 52
reference port choice, 48
S-channel bundle group (dynamic), 60
S-channel bundle group (static), 60
simple multichassis link aggregation, 54
simple multichassis link aggregation (S-MLAG), 77
static mode, 48
traffic redirection, 72
traffic redirection restrictions, 73
Ethernet subinterface, 1, See also Ethernet interface,
Layer 2 Ethernet subinterface, Layer 3 Ethernet subinterface
  basic settings, 4
display, 21
MAC address (Layer 3), 20
maintain, 21
MTU setting (Layer 3), 20
packet statistics, 21
ETS parameter (LLDP), 307
EVB
  loop detection protection action (S-channel interface), 163
external
  Ethernet interface external loopback testing, 9
F
failover
  DR system auto-recovery, 349
  DRNI failover, 336
fast
  MAC address table ARP fast update, 38
FC interface
  Layer 2 Ethernet interface change, 16
FCoE
  LLDP APP parameters, 305
  LLDP DCBX configuration, 317
  LLDP DCBX version, 305
fiber port
  Ethernet interface fiber port (Layer 2), 17
flow control
  Ethernet interface generic flow control, 10
  Ethernet interface PFC, 11
forcing
  Ethernet interface fiber port (Layer 2), 17
format
  LLDP frame encapsulation (Ethernet II), 287
  LLDP frame encapsulation (SNAP), 287
  LLDP frame encapsulation format, 300
  LLDP management address encoding format, 298
  PBB frame format, 277
forwarding
  Layer 2 forwarding configuration (cut-through), 334
  MAC address table frame forwarding rule, 34
  MST forwarding port state, 114
  PBB frame forwarding, 279
  spanning tree forward delay timer, 125
  STP BPDU forwarding, 105
  STP forward delay timer, 105
frame
  Ethernet interface jumbo frame support, 6
  Layer 2 forwarding configuration (cut-through), 334
  LLDP ARP entry generation, 311
  LLDP frame encapsulation format, 300
  LLDP source MAC address, 310
  loop detection (Ethernet frame header), 160
  loop detection (inner frame header), 160
  loop detection interval, 161
  MAC address learning, 27
  MAC address table blackhole entry, 30
  MAC address table configuration, 27, 28, 40
  MAC address table entry configuration, 29
  MAC address table frame forwarding rule, 34
  MAC address table multiport unicast entry, 31
  MAC Information configuration, 42, 43
  MSTP BPDU protocol frames, 109
  PBB frame forwarding, 279
  port-based VLAN frame handling, 172
  PVST BPDU protocol frames, 108, 108
  QinQ CVLAN Ethernet frame header tag, 245
  QinQ implementation, 246
  QinQ SVLAN Ethernet frame header tag, 245
  RSTP BPDU protocol frames, 106
  spanning tree port mode configuration, 133
  STP BPDU protocol frames, 97
  STP TCN BPDU protocol frames, 97
  VLAN frame encapsulation, 168
generic flow control (Ethernet interface), 10
Generic VLAN Registration Protocol. Use GVRP
global
  Ethernet link aggregation load sharing mode set, 70
  loop detection enable, 162
  loop detection protection action, 163
  MAC address learning disable, 32
  MAC address table multiport unicast entry configuration, 31
  spanning tree BPDU guard enable, 142
  group
  dynamic link aggregation, 50
  Ethernet link aggregate group Selected ports min/max, 64
  Ethernet link aggregation, 56
  Ethernet link aggregation group, 46
  Ethernet link aggregation group (Layer 2 static), 57, 57
  Ethernet link aggregation group (Layer 2), 57
  Ethernet link aggregation group (Layer 3 dynamic), 59
  Ethernet link aggregation group (Layer 3 static), 58
  Ethernet link aggregation group (Layer 3), 58
  Ethernet link aggregation group load sharing, 69
  Ethernet link aggregation LACP, 50
  Ethernet link aggregation load sharing mode, 54, 69
  Ethernet link aggregation member port state, 47
  port isolation configuration (multiple isolation groups), 95
  S-channel bundle group (dynamic), 60
  S-channel bundle group (static), 60
  VLAN group configuration, 182
GVRP
  MVRP compatibility, 234
H
  hello
  spanning tree timer, 125
  STP timer, 105
host
  voice VLAN host+IP phone connection (in series), 214
  voice VLAN IP phone+device connection, 215
hybrid port
  port-based VLAN assignment (hybrid port), 174
I
  identifying
  voice VLAN IP phone identification (LLDP), 214
voice VLAN IP phone identification (OUI address), 213

ignored VLAN
   Layer 2 aggregate interface, 62
implementing
   0:2 VLAN mapping, 257
   1:1 VLAN mapping, 257, 258
   1:2 VLAN mapping, 257, 259
   2:2 VLAN mapping, 257, 259
   2:3 VLAN mapping, 257
   M:1 VLAN mapping, 257, 258
MSTP device, 115
QinQ, 246

inloopback interface
   configuration, 24
   display, 24
   maintain, 24
interface
   bulk configuration, 25, 25
   configuration (inloopback), 23, 24
   configuration (loopback), 23, 23
   configuration (null), 23, 23
   Ethernet aggregate interface, 61
   Ethernet aggregate interface (description), 61
   Ethernet aggregate interface (MAC address), 62
   Ethernet link aggregate interface default settings, 69
   Ethernet link aggregate interface shutdown, 68
   Ethernet link aggregation edge aggregate interface, 54, 65
   Ethernet link aggregation member port state (port speed), 63
   Layer 2 Ethernet aggregate interface (ignored VLAN), 62
   Layer 3 aggregate interface configuration (MTU), 63
   Layer 3 aggregate subinterface packet statistics, 68
   LLDP neighbor aging configuration, 303
   LLDP neighbor validation configuration, 302
   simple multichassis link aggregation, 54
   simple multichassis link aggregation (S-MLAG), 77
   internal
      Ethernet interface internal loopback testing, 9
   interval
data restoration interval, 349
   DR keepalive interval, 346
   Ethernet link aggregation LACP long timeout, 51
   Ethernet link aggregation LACP short timeout, 51
   loop detection, 161, 164
   MAC change notification interval, 43
IP addressing
   IP subnet-based VLAN configuration, 180, 187
   super VLAN configuration, 192, 192, 194
   super VLAN interface configuration, 193
   voice VLAN configuration, 213, 218, 223
IP phone
   voice VLAN assignment mode+IP phone cooperation, 216
   voice VLAN host+IP phone connection (in series), 214
   voice VLAN identification (LLDP), 214
   voice VLAN identification (OUI address), 213
   voice VLAN information advertisement, 214
   voice VLAN IP phone access method, 214
   voice VLAN IP phone+device connection, 215
IP subnet-based VLAN
   configuration, 180, 187
IPP
   failure handling mechanism, 339
   IPP specification, 347
   short DRCP timeout timer, 348
isolating
   ports. See port isolation
IST
   MST region, 112
J
   jumbo frame support (Ethernet interface), 6
K
   keepalive
      DR keepalive interval, 346
      DR keepalive packet parameters, 345
      DR keepalive settings, 344
      DR keepalive timeout timer, 346
      DRNI keepalive, 336
      keepalive hold timer, 348
key
   Ethernet link aggregation operational key, 47
L
   L2PT
      configuration, 323, 325, 327
      display, 326
      enable, 325
      enable restrictions, 325
      how it works, 324
      LACP configuration, 328
      maintain, 326
STP configuration, 327
tunneled packet destination multicast MAC address, 326

L2VPN
PBB enable, 280

LACP
dynamic link aggregation, 50
Ethernet link aggregation, 50
L2PT for LACP configuration, 328

LAN
Virtual Local Area Network. Use VLAN
LAN switching
1:1 VLAN mapping configuration, 261, 267
1:2 VLAN mapping configuration, 266, 273
2:2 VLAN mapping configuration, 267, 273
default link-aggregation load sharing ignored packet fields, 70
DR group configuration, 350
DRNI configuration, 335, 350
DRNI with PVST configuration, 157
dynamic link aggregation, 50
Ethernet aggregate interface, 61
Ethernet aggregate interface (description), 61
Ethernet aggregate interface (ignored VLAN), 62
Ethernet link aggregate group Selected ports min/max, 64
Ethernet link aggregate interface (expected bandwidth), 65
Ethernet link aggregate interface (Layer 2 edge), 85
Ethernet link aggregate interface default settings, 69
Ethernet link aggregate interface shutdown, 68
Ethernet link aggregation (Layer 2 dynamic), 80
Ethernet link aggregation (Layer 2 static), 79
Ethernet link aggregation (Layer 3 dynamic), 87
Ethernet link aggregation (Layer 3 static), 86
Ethernet link aggregation (static mode), 48
Ethernet link aggregation BFD configuration restrictions, 66
Ethernet link aggregation configuration, 46, 55, 79
Ethernet link aggregation display, 78
Ethernet link aggregation edge aggregate interface, 54, 65
Ethernet link aggregation group, 56
Ethernet link aggregation group (dynamic dynamic), 57
Ethernet link aggregation group (Layer 2 static), 57
Ethernet link aggregation group (Layer 2), 57
Ethernet link aggregation group (Layer 3 dynamic), 59
Ethernet link aggregation group (Layer 3 static), 58
Ethernet link aggregation group load sharing, 69
Ethernet link aggregation group load sharing mode, 69
Ethernet link aggregation group restrictions, 56
Ethernet link aggregation LACP, 50
Ethernet link aggregation load sharing (Layer 2), 82
Ethernet link aggregation load sharing (Layer 3), 89
Ethernet link aggregation load sharing mode, 54
Ethernet link aggregation local-first load sharing, 71
Ethernet link aggregation maintain, 78
Ethernet link aggregation traffic redirection, 72
Ethernet link aggregation traffic redirection restrictions, 73
IP subnet-based VLAN configuration, 180, 187
L2PT configuration, 323, 327
L2PT display, 326
L2PT enable, 325
L2PT enable restrictions, 325
L2PT for LACP configuration, 328
L2PT for STP configuration, 327
L2PT maintain, 326
Layer 3 aggregate subinterface packet statistics, 68
LLDP basic concepts, 286
LLDP basic configuration, 293, 312
LLDP CDP compatibility, 301
LLDP configuration, 286, 292, 312
LLDP configuration (CDP-compatible), 316
LLDP DCBX configuration, 317
LLDP display, 311
LLDP protocols and standards, 292
loop detection configuration, 160, 162, 164
M:1 VLAN mapping configuration, 261, 267
M:1 VLAN mapping restrictions (dynamic IP address assignment), 261
M:1 VLAN mapping restrictions (static IP address assignment), 264
MAC address table configuration, 27, 28, 40
MAC address table display, 40
MAC Information configuration, 42, 43
MAC-based VLAN assignment (dynamic), 178
MAC-based VLAN assignment (static), 178
MAC-based VLAN assignment configuration restrictions (dynamic), 178
MAC-based VLAN configuration, 175, 185
MAC-based VLAN configuration (server-assigned), 180
MRP implementation, 228
MST region, 122
MSTP configuration, 150
MVRP configuration, 228, 231, 234
MVRP configuration restrictions, 231
MVRP display, 234
MVRP GVRP compatibility, 234
MVRP maintain, 234
MVRP protocols and standards, 231
MVRP registration mode setting, 232
MVRP timer set, 233
PBB configuration, 276, 280, 283
PBB configuration restrictions, 280
PBB data encapsulation type configuration, 282
PBB display, 283
PBB downlink port, 281
PBB frame format, 277
PBB frame forwarding, 279
PBB L2VPN enable, 280
PBB maintain, 283
PBB protocols and standards, 279
PBB uplink port, 281
PBB VSI B-VLAN configuration, 281
PBB VSI creation, 280
port bridging on Layer 2 aggregate interface, 75
port isolation configuration, 94
port isolation configuration (multiple isolation groups), 95
port isolation display, 94
port isolation group assignment (multiple ports), 94
port-based VLAN assignment (access port), 173
port-based VLAN assignment (hybrid port), 174
port-based VLAN assignment (trunk port), 173
port-based VLAN configuration, 171
private VLAN configuration, 197, 198, 200
private VLAN configuration restrictions, 198
private VLAN display, 200
private VLAN promiscuous port configuration, 200
private VLAN trunk promiscuous port configuration, 203
private VLAN trunk promiscuous+secondary port configuration, 206
protocol-based VLAN configuration, 181, 188
PVST configuration, 154
QinQ basic configuration, 251
QinQ configuration, 245, 251
QinQ configuration restrictions, 247
QinQ display, 250
QinQ implementation, 246
QinQ protocols and standards, 247
QinQ SVLAN tag 802.1p priority, 249
QinQ VLAN tag TPID value, 248
QinQ VLAN transparent transmission configuration, 253
secondary VLAN Layer 3 communication configuration, 210
service loopback group configuration, 332, 333
service loopback group display, 333
simple multichassis link aggregation, 54
simple multichassis link aggregation (S-MLAG), 77
S-MLAG (Layer 2 dynamic), 91
spanning tree configuration, 97, 150
spanning tree Digest Snooping, 136, 137
spanning tree display, 149
spanning tree maintain, 149
spanning tree No Agreement Check, 138, 140
spanning tree protection configuration, 142
spanning tree TC Snooping, 140
super VLAN configuration, 192, 192, 194
super VLAN display, 193
super VLAN interface configuration, 193
super VLAN sub-VLAN creation, 192
troubleshooting PBB, 285
troubleshooting PBB customer frames cannot be transmitted, 285
VLAN basic configuration, 169
VLAN configuration, 168, 183
VLAN configuration restrictions, 178
VLAN display, 183
VLAN group configuration, 182
VLAN interface, 170
VLAN maintain, 183
VLAN mapping configuration, 255, 260, 267
VLAN mapping display, 267
VLAN port-based configuration, 183
VLAN protocols and standards, 169
voice VLAN advertisement (CDP), 222
voice VLAN advertisement (LLDP), 222
voice VLAN assignment mode configuration (automatic), 223
voice VLAN assignment mode configuration (manual), 225
voice VLAN display, 223
voice VLAN LLDP automatic IP phone discovery enable, 221
voice VLAN port operation configuration (automatic assignment), 219
voice VLAN port operation configuration (manual assignment), 220
voice VLAN port operation configuration restrictions (automatic assignment), 219
voice VLAN port operation configuration restrictions (manual assignment), 220
Layer 2
  distributed relay, 335, 350
  Distributed Resilient Network Interconnect, 335, 350
  Ethernet interface bridging enable, 19
  Ethernet interface cable connection, 19
  Ethernet interface change to FC interface, 16
  Ethernet interface configuration, 1, 15
  Ethernet interface connection distance, 20
  Ethernet interface fiber port, 17
  Ethernet interface fiber port restrictions, 18
  Ethernet interface MDIX mode, 18
  Ethernet interface storm control configuration, 15
  Ethernet interface storm control configuration restrictions, 16
  Ethernet link aggregate interface (Layer 2 edge), 85
  Ethernet link aggregation (Layer 2 dynamic), 80
  Ethernet link aggregation (Layer 2 static), 79
  Ethernet link aggregation load sharing, 82
  Ethernet link aggregation member port state (port speed), 63
  forwarding configuration (cut-through), 334
  L2PT configuration, 325
  L2PT tunneled packet destination multicast MAC address, 326
  LLDP basic configuration, 312
  LLDP configuration, 312
  LLDP group-based WRR queuing, 308
  LLDP trapping, 309
  LLDP+DCBX TLV advertisement, 304
  LLDP-MED trapping, 309
  loop detection protection action (Layer 2 aggregate interface), 163
  loop detection protection action (Layer 2 Ethernet interface), 163
  loop detection protection action (S-channel aggregate interface), 163
  loop detection protection action (S-channel bundle interface), 163
  loop detection protection action (S-channel interface), 163
  PBB configuration, 276, 280, 283
  PBB data encapsulation type configuration, 282
  PBB downlink port, 281
  PBB frame format, 277
  PBB L2VPN enable, 280
  PBB uplink port, 281
  PBB VSI B-VLAN configuration, 281
  PBB VSI creation, 280
  port bridging on Layer 2 aggregate interface, 75
  S-MLAG (Layer 2 dynamic), 91
  VLAN basic configuration, 169
  VLAN configuration, 168, 183
  voice VLAN configuration, 213, 218, 223
Layer 2 Protocol Tunneling. Use L2PT
Layer 3
  aggregate interface configuration (MTU), 63
  aggregate subinterface packet statistics, 68
  Ethernet aggregate interface, 61
  Ethernet aggregate interface (description), 61
  Ethernet aggregate interface (MAC address), 62
  Ethernet interface configuration, 1, 20
  Ethernet interface MAC address, 20
  Ethernet interface MTU setting, 20
  Ethernet link aggregate group Selected ports min/max, 64
  Ethernet link aggregate interface (expected bandwidth), 65
  Ethernet link aggregate interface default settings, 69
  Ethernet link aggregate interface shutdown, 68
  Ethernet link aggregation (Layer 3 dynamic), 87
  Ethernet link aggregation (Layer 3 static), 86
  Ethernet link aggregation configuration, 46, 55, 79
  Ethernet link aggregation edge aggregate interface, 54, 65
  Ethernet link aggregation group, 56, 58
  Ethernet link aggregation group load sharing, 69
  Ethernet link aggregation group load sharing mode, 69
  Ethernet link aggregation load sharing, 89
  Ethernet link aggregation local-first load sharing, 71
  Ethernet link aggregation member port state (port speed), 63
  Ethernet link aggregation traffic redirection, 72
  Ethernet subinterface configuration, 20
Ethernet subinterface MAC address, 20
Ethernet subinterface MTU setting, 20
IP subnet-based VLAN configuration, 180
LAN switching LAN switching VLAN interface, 170
LLDP ARP entry generation, 311
LLDP basic configuration, 312
LLDP configuration, 312
LLDP trapping, 309
LLDP-MED trapping, 309
port-based VLAN assignment (access port), 173
port-based VLAN assignment (hybrid port), 174
port-based VLAN assignment (trunk port), 173
private VLAN configuration, 200
private VLAN promiscuous port configuration, 200
private VLAN trunk promiscuous port configuration, 203
private VLAN trunk promiscuous+secondary port configuration, 206
protocol-based VLAN configuration, 181
secondary VLAN Layer 3 communication configuration, 210
super VLAN configuration, 194
voice VLAN configuration, 213, 218, 223
learning
loop detection no-learning action, 161
MAC address, 27
MAC address learning disable, 32
MAC address table learning limit, 34
MAC address table learning priority, 34
MST learning port state, 114
legacy
spanning tree port mode, 133
spanning tree port path cost calculation, 128
link
aggregation. See link aggregation
DRNI with PVST configuration, 157
Ethernet interface link flapping protection, 8
Ethernet interface link mode, 5
intra-portal link (IPL), 335
Link Layer Discovery Protocol. Use LLDP
MSTP configuration, 150
PVST configuration, 154
spanning tree configuration, 97, 118, 150
spanning tree hello time, 125
spanning tree port link type configuration, 132
distributed relay, 335, 350, 350
Distributed Resilient Network Interconnect, 335, 350
Ethernet link aggregation. See Ethernet link aggregation
LLDP
802.1p-to-local priority mapping, 307
advertisable TLV configuration, 295
agent, 286
APP parameter configuration, 305
APP parameter configuration restrictions, 306
ARP entry generation, 311
basic concepts, 286
basic configuration, 293, 312
bridge mode configuration, 293
CDP compatibility configuration, 301
CDP-compatible configuration, 316
configuration, 286, 292, 312
DCBX configuration, 303, 317
DCBX version configuration, 305
disabling PVID inconsistency check, 300
display, 311
enable, 293
ETS parameter configuration, 307
frame encapsulation (Ethernet II), 287
frame encapsulation (SNAP), 287
frame encapsulation format, 300
frame format, 287
frame reception, 292
frame transmission, 291
group-based WRR queuing, 308
how it works, 291
LLDP+DCBX TLV advertisement, 304
LLDPDU management address TLV, 291
LLDPDU TLV types, 288
LLDPDU TLVs, 288
LLDP-MED trapping configuration, 309
management address configuration, 298
management address encoding format, 298
neighbor aging configuration, 302, 303
neighbor validation and aging, 302
neighbor validation configuration, 302, 302
operating mode (disable), 291
operating mode (Rx), 291
operating mode (Tx), 291
operating mode (TxRx), 291
operating mode set, 294
parameter set, 299
PFC parameter configuration, 309
polling enable, 295
protocols and standards, 292
reinitialization delay, 294
source MAC address, 310
trapping configuration, 309
voice VLAN advertisement, 222
voice VLAN information advertisement to IP phones, 214
voice VLAN IP phone identification, 214
voice VLAN IP phone identification method, 213
voice VLAN LLDP automatic IP phone discovery enable, 221

LLDPDU
LLDP basic configuration, 293, 312
LLDP configuration, 286, 292, 312
LLDP parameters, 299
management address configuration, 298
management address encoding format, 298
management address TLV, 291
TLV basic management types, 288
TLV LLDP-MED types, 288
TLV organization-specific types, 288

load balancing
service loopback group configuration, 332, 333

load sharing
default link-aggregation load sharing ignored packet fields, 70
Ethernet link aggregation group configuration, 69
Ethernet link aggregation group load sharing, 54
Ethernet link aggregation load sharing (Layer 2), 82
Ethernet link aggregation load sharing (Layer 3), 89
Ethernet link aggregation load sharing algorithm settings, 72
Ethernet link aggregation load sharing mode, 69
Ethernet link aggregation load sharing mode for MAC-in-MAC traffic (global), 72
Ethernet link aggregation local-first load sharing, 71
Ethernet link aggregation packet type-based load sharing, 54
Ethernet link aggregation per-flow load sharing, 54
Ethernet link aggregation per-packet load sharing, 54
local
Ethernet link aggregation local-first load sharing, 71

logging
spanning tree TC BPDU event logging (PVST mode), 148

loop
DRNI with PVST configuration, 157
MSTP configuration, 150
PVST configuration, 154
spanning tree configuration, 97, 118, 150
spanning tree loop guard, 143

loop detection
configuration, 160, 162, 164
display, 164
enable, 162
interval, 161
interval setting, 164
mechanisms, 160
port status auto recovery, 161
protection action setting, 163
protection action setting (Layer 2 aggregate interface), 163
protection action setting (S-channel aggregate interface), 163
protection action setting (S-channel bundle interface), 163
protection actions, 161

loopback
Ethernet interface loopback testing, 9

loopback interface
configuration, 23
display, 24
maintain, 24

M
M:1 VLAN mapping
application scenario, 255, 255
ARP detection (dynamic IP address assignment), 262
ARP snooping (static IP address assignment), 264
configuration, 261, 267
configuration (dynamic IP address assignment), 261
configuration (static IP address assignment), 264
configuration restrictions (dynamic IP address assignment), 261
configuration restrictions (static IP address assignment), 264
customer-side port (dynamic IP address assignment), 262
customer-side port (static IP address assignment), 264
DHCP snooping (dynamic IP address assignment), 262
implementation, 257, 258
network-side port (dynamic IP address assignment), 263
network-side port (static IP address assignment), 265
MAC
  PBB configuration, 280, 283
MAC address
  DR system MAC, 342
MAC address table
  address learning, 27
  address synchronization, 35
  ARP fast update enable, 38
  blackhole entry, 30
  configuration, 27, 28, 40
  display, 40
  dynamic aging timer, 33
  entry configuration, 29
  entry configuration (global), 29
  entry configuration (on interface), 30
  entry creation, 27
  entry types, 27
  frame forwarding rule, 34
  learning limit setting set, 34
  learning priority assignment, 34
  MAC address learning disable, 32
  MAC address move suppression, 37
  manual entries, 27
  move notification, 37
  multiport unicast entry, 31
  SNMP notification enable, 39
  static source check enable, 38
MAC addressing
  Ethernet aggregate interface, 62
  Ethernet interface MAC address (Layer 3), 20
  Ethernet subinterface MAC address (Layer 3), 20
  L2PT tunneled packet destination multicast
  MAC address, 326
  LLDP source MAC address, 310
MAC-based VLAN
  assignment (dynamic), 176, 178
  assignment (server-assigned), 177
  assignment (static), 175, 178
  configuration restrictions, 178
MAC-based VLAN configuration, 175, 185
MAC-based VLAN configuration
  (server-assigned), 180
  VLAN frame encapsulation, 168
MAC authentication
  VLAN group configuration, 182
MAC Information
  change notification interval, 43
  configuration, 42, 43
  configuration restrictions, 44
  enable, 42
  mode configuration, 42
  queue length setting, 43
MAC relay (LLDP agent), 286
MAC-based VLAN
  assignment (dynamic), 178
  assignment (static), 178
  configuration, 175, 185
  configuration (server-assigned), 180
  dynamic assignment, 176
  dynamic assignment configuration restrictions, 178
  server-assigned, 177
  static assignment, 175
MAC-in-MAC
  Ethernet link aggregation group load sharing
  mode for MAC-in-MAC traffic, 72
  PBB configuration, 276
MAD
  data restoration interval, 349
  excluding interface from shutdown action by
  DRNI MAD (F2611 and later), 344
  excluding interface from shutdown action by
  DRNI MAD (Release 2609), 344
maintaining
  DRNI, 350
  Ethernet interface, 21
  Ethernet link aggregation, 78
  Ethernet subinterface, 21
  interface, 24
  L2PT, 326
  MVRP, 234
  PBB, 283
  spanning tree, 149
  VLAN, 183
management address
  LLDP encoding format, 298
manual
  voice VLAN assignment mode, 216
  voice VLAN assignment mode configuration, 225
  voice VLAN port operation configuration, 220
mapping
  1:1 VLAN mapping, 255
  1:2 VLAN mapping, 256
  2:2 VLAN mapping, 256
  M:1 VLAN mapping, 255
MSTP VLAN-to-instance mapping table, 112
master
MSTP master port, 113
max age timer (STP), 105
maximum transmission unit. Use MTU mCheck
global performance, 135
interface view performance, 136
spanning tree, 135
MDI mode (Ethernet interface), 18
MDIX mode (Ethernet interface), 18
mechanism
DRCP operating mechanism, 336
DRNI failover mechanism, 336
DRNI failure handling mechanism, 339
DRNI keepalive mechanism, 336
MED (LLDP-MED trapping), 309
message
MRP JoinEmpty, 228
MRP JoinIn, 228
MRP Leave, 228
MRP LeaveAll, 228
MRP New, 228
MRP timers, 230
MIB
LLDP basic configuration, 293, 312
LLDP configuration, 286, 292, 312
mode
Ethernet interface Auto MDIX (Layer 2), 18
Ethernet interface link, 5
Ethernet interface MDI (Layer 2), 18
Ethernet interface MDIX (Layer 2), 18
Ethernet link aggregation dynamic, 48
Ethernet link aggregation LACP operation active, 50
Ethernet link aggregation LACP operation passive, 50
Ethernet link aggregation load sharing, 54
Ethernet link aggregation static, 48, 48
LLDP customer bridge, 293
LLDP disable, 291, 294
LLDP Rx, 291, 294
LLDP service bridge, 293
LLDP Tx, 291, 294
LLDP TxRx, 291, 294
MAC Information syslog, 42
MAC Information trap, 42
MVRP registration, 232
MVRP registration fixed, 231
MVRP registration forbidden, 231
MVRP registration normal, 231
spanning tree mCheck, 135
spanning tree MSTP, 121
spanning tree PVST, 121
spanning tree RSTP, 121
spanning tree STP, 121
voice VLAN assignment automatic, 215
voice VLAN assignment manual, 216
voice VLAN port operation normal, 217
voice VLAN port operation security, 217
modifying
MAC address table blackhole entry, 30
MAC address table entry (global), 29
MAC address table entry (on interface), 30
MAC address table multiport unicast entry, 31
moving
MAC address table move notification, 37
MQC
LLDP 802.1p-to-local priority mapping, 307
MRP
implementation, 228
messages, 228
MVRP configuration, 228, 231, 234
timers, 230
MST
region max hops, 124
MSTI
calculation, 114
MRP, 228
MST instance, 112
MSTP, 97, See also STP
basic concepts, 111
CIST, 112
CIST calculation, 114
common root bridge, 113
configuration, 121, 150
CST, 112
device implementation, 115
feature enable, 134
features, 109
how it works, 114
IST, 112
mode set, 121
MST region, 112
MST region configuration, 122
MSTI, 112
MSTI calculation, 114
port roles, 113
port states, 114
protocol frames, 109
protocols and standards, 117
rapid transition, 115
regional root, 112
relationships, 109
spanning tree max age timer, 125
spanning tree port mode configuration, 133
VLAN-to-instance mapping table, 112
MTU
  Ethernet subinterface MTU setting (Layer 3), 20
  Layer 3 Ethernet aggregate interface, 63
multicast
  L2PT tunneled packet destination multicast MAC address, 326
multichassis
  distributed relay, 335, 350, 350
  Distributed Resilient Network Interconnect, 335, 350
multiple
  Multiple Registration Protocol. Use MRP
  VLAN Registration Protocol. Use MVRP
Multiple Spanning Tree Protocol. Use MSTP
multiport unicast entry (MAC address table), 27, 31
MVRP
  configuration, 228, 231, 234
  configuration restrictions, 231
  display, 234
  enable, 232
  GVRP compatibility, 234
  maintain, 234
  MRP implementation, 228
  protocols and standards, 231
  registration mode setting, 232
  registration modes, 231
  timer set, 233
N
network
  1:1 VLAN mapping configuration, 261, 267
  1:2 VLAN mapping configuration, 266, 273
  2:2 VLAN mapping configuration, 267, 273
  common Ethernet interface settings configuration, 2
  disabling the device to reactivate the shutdown edge ports, 148
  DRNI network model, 335
  DRNI with PVST configuration, 157
  dynamic link aggregation, 50
  Ethernet interface basic settings, 4
  Ethernet interface bridging enable (Layer 2), 19
  Ethernet interface cable connection (Layer 2), 19
  Ethernet interface combine (10-GE > 40-GE), 2
  Ethernet interface configuration (Layer 2), 15
  Ethernet interface configuration (Layer 3), 20
  Ethernet interface connection distance (Layer 2), 20
  Ethernet interface dampening, 7
  Ethernet interface fiber port (Layer 2), 17
  Ethernet interface generic flow control, 10
  Ethernet interface jumbo frame support, 6
  Ethernet interface link flapping protection, 8
  Ethernet interface link mode, 5
  Ethernet interface loopback testing, 9
  Ethernet interface MAC address (Layer 3), 20
  Ethernet interface MDIX mode (Layer 2), 18
  Ethernet interface MTU setting (Layer 3), 20
  Ethernet interface PFC, 11
  Ethernet interface PFC thresholds, 12
  Ethernet interface physical state change suppression, 6
  Ethernet interface split (40-GE), 2
  Ethernet interface statistics polling interval, 13
  Ethernet interface storm control (Layer 2), 15
  Ethernet interface storm suppression, 14
  Ethernet link aggregate interface (Layer 2 edge), 85
  Ethernet link aggregation (Layer 2 dynamic), 80
  Ethernet link aggregation (Layer 2 static), 79
  Ethernet link aggregation (Layer 3 dynamic), 87
  Ethernet link aggregation (Layer 3 static), 86
  Ethernet link aggregation (static mode), 48
  Ethernet link aggregation aggregate interface types, 46
  Ethernet link aggregation configuration types, 47
  Ethernet link aggregation edge aggregate interface, 54
  Ethernet link aggregation LACP, 50
  Ethernet link aggregation load sharing (Layer 2), 82
  Ethernet link aggregation load sharing (Layer 3), 89
  Ethernet link aggregation member port state, 49, 53
  Ethernet link aggregation modes, 48
  Ethernet link aggregation operational key, 47
  Ethernet link aggregation reference port, 52
  Ethernet link aggregation reference port choice, 48
  Ethernet link aggregation reference port speed, 67
  Ethernet subinterface basic settings, 4
  Ethernet subinterface configuration (Layer 3), 20
  Ethernet subinterface MAC address (Layer 3), 20
spanning tree Digest Snooping, 136, 137
spanning tree dispute guard, 146
spanning tree edge port, 128
spanning tree inconsistent PVID protection disable, 136
spanning tree loop guard, 143
spanning tree mode set, 121
spanning tree No Agreement Check, 138, 140
spanning tree port link type, 132
spanning tree port mode, 133
spanning tree port path cost, 128, 131
spanning tree port priority, 132
spanning tree port role restriction, 144
spanning tree port state transition, 133
spanning tree priority, 124
spanning tree protection, 142
spanning tree root bridge, 123
spanning tree root bridge (device), 123
spanning tree root guard, 143
spanning tree secondary root bridge (device), 124
spanning tree SNMP notification (new-root election, topology change events), 149
spanning tree switched network diameter, 125
spanning tree TC BPDU event logging (PVST mode), 148
spanning tree TC Snooping, 140
spanning tree TC-BPDU guard, 145
spanning tree TC-BPDU transmission restriction, 144
STP algorithm calculation, 100
STP basic concepts, 99
STP path cost, 100
super VLAN configuration, 192, 194
super VLAN interface configuration, 193
super VLAN sub-VLAN creation, 192
VLAN basic configuration, 169
VLAN group configuration, 182
VLAN interface, 170
VLAN mapping 1:1 implementation, 258
VLAN mapping 1:2 implementation, 259
VLAN mapping 2:2 implementation, 259
VLAN mapping M:1 implementation, 258
VLAN port-based configuration, 183
voice VLAN advertisement (CDP), 222
voice VLAN advertisement (LLDP), 222
voice VLAN assignment mode, 215
voice VLAN assignment mode configuration (automatic), 223
voice VLAN assignment mode configuration (manual), 225
voice VLAN configuration, 223
voice VLAN host+IP phone connection (in series), 214
voice VLAN information advertisement to IP phones, 214
voice VLAN IP phone access method, 214
voice VLAN IP phone identification (LLDP), 214
voice VLAN IP phone identification (OUI address), 213
voice VLAN IP phone+device connection, 215
voice VLAN LLDP automatic IP phone discovery enable, 221
voice VLAN port operation configuration (automatic assignment), 219
voice VLAN port operation configuration (manual assignment), 220
voice VLAN port operation mode, 217
voice VLAN traffic QoS priority settings, 218

network management
Ethernet interface configuration, 1
Ethernet link aggregation configuration, 46, 55, 79
interface bulk configuration, 25, 25
interface configuration (inloopback), 23
interface configuration (loopback), 23
interface configuration (null), 23
L2PT configuration, 323, 325, 327
LLDP basic concepts, 286
LLDP configuration, 286, 292, 312
loop detection, 160
loop detection configuration, 162, 164
MAC address table configuration, 27, 28, 40
MAC Information configuration, 42
MVRP, 228, 231, 234
PBB configuration, 276, 280, 283
PBB network model, 276
port isolation configuration, 94
private VLAN configuration, 197, 198, 200
QinQ configuration, 245, 251
service loopback group configuration, 332
spanning tree configuration, 97, 118, 150
super VLAN configuration, 192
VLAN configuration, 168, 183
VLAN mapping configuration, 255, 260, 267
voice VLAN configuration, 213, 218

No Agreement Check (spanning tree), 138, 140
no-learning action (loop detection), 161
normal
voice VLAN operation mode, 217
notifying
MAC address table move notification, 37
MAC address table SNMP notification, 39
MAC Information change notification interval, 43
null interface
  configuration, 23, 23
display, 24
  maintain, 24
O
  operational key (Ethernet link aggregation), 47
organization-specific LLDPDU TLV types, 288
OUI
  voice VLAN IP phone identification (OUI address), 213
  voice VLAN IP phone identification method, 213
outputting
  spanning tree port state transition information, 133
P
P/A transition (STP), 116
packet
  1:1 VLAN mapping configuration, 261, 267
  1:2 VLAN mapping configuration, 266, 273
  2:2 VLAN mapping configuration, 267, 273
default link-aggregation load sharing ignored packet fields, 70
  DR keepalive packet parameters, 345
  DRCPDU, 336
Ethemet link aggregation group BFD, 66
  Ethernet link aggregation packet type-based load sharing, 54
L2PT configuration, 323, 325, 327
  L2PT for LACP configuration, 328
  L2PT for STP configuration, 327
L2PT tunneled packet destination multicast MAC address, 326
LLDP CDP compatibility, 301
LLDP DCBX configuration, 317
LLDP PFC parameters, 309
M:1 VLAN mapping configuration, 261, 267
  M:1 VLAN mapping configuration (dynamic IP address assignment), 261
  M:1 VLAN mapping configuration (static IP address assignment), 264
port bridging on Layer 2 aggregate interface, 75
  service loopback group configuration, 332, 333
  transparent LACPDU transmission on VPLS network, 76
  VLAN mapping configuration, 255, 260, 267
parameter
LLDP APP configuration, 305
LLDP DCBX configuration, 305
LLDP ETS configuration, 307
LLDP PFC configuration, 309
  spanning tree timeout factor, 127
PBB
  configuration, 276, 280, 283
  configuration restrictions, 280
data encapsulation type configuration, 282
display, 283
downlink port configuration, 281
  frame format, 277
  frame forwarding, 279
L2VPN enable, 280
  maintain, 283
network model, 276
  protocols and standards, 279
terminology, 277
troubleshoot, 285
  troubleshooting customer frames cannot be transmitted, 285
uplink port configuration, 281
VSI B-VLAN configuration, 281
VSI creation, 280
PE
  L2PT configuration, 323, 325, 327
  L2PT for LACP configuration, 328
  L2PT for STP configuration, 327
per-flow load sharing, 54
performing
  spanning tree mCheck, 135
  spanning tree mCheck globally, 135
  spanning tree mCheck in interface view, 136
per-packet load sharing, 54
Per-VLAN Spanning Tree Protocol. Use PVST
PFC
  setting PFC thresholds, 12
  PFC (Ethernet interface), 11
PFC priority (LLDP), 309
physical
  Ethernet interface physical state change suppression, 6
polling
  Ethernet interface statistics polling interval, 13
  LLDP enable, 295
port
  aggregate interface (MAC address), 62
  DR group configuration, 350
  DRNI configuration, 335, 350
dynamic link aggregation, 50
  Ethernet aggregate interface, 61
MAC address learning, 27
MAC address table blackhole entry, 30
MAC address table configuration, 27, 28, 40
MAC address table entry configuration, 29
MAC address table multiport unicast entry, 31
MAC Information configuration, 42, 43
MST port roles, 113
MST port states, 114
MVRP application, 228, 231, 234
MVRP timer set, 233
PBB downlink port, 281
PBB uplink port, 281
PVST BPDU guard, 146
QinQ implementation, 246
RSTP network convergence, 106
S-channel bundle group, 60
S-channel bundle group (dynamic), 60
S-channel bundle group (static), 60
service loopback group configuration, 332, 333
simple multichassis link aggregation, 54
S-MLAG (Layer 2 dynamic), 91
spanning tree BPDU drop, 145
spanning tree BPDU guard, 142
spanning tree BPDU transmission rate, 127
spanning tree BPDU transparent transmission (on port), 148
spanning tree dispute guard, 146
spanning tree edge port configuration, 128
spanning tree forward delay timer, 125
spanning tree loop guard, 143
spanning tree mCheck, 135
spanning tree path cost calculation standard, 128
spanning tree path cost configuration, 128, 131
spanning tree port link type configuration, 132
spanning tree port mode configuration, 133
spanning tree port priority configuration, 132
spanning tree port role restriction, 144
spanning tree port state transition output, 133
spanning tree root guard, 143
spanning tree TC-BPDU guard, 145
spanning tree TC-BPDU transmission restriction, 144
STP designated port, 99
STP edge port rapid transition, 115
STP port state, 99
STP rapid transition, 115
STP root port, 99
STP root port rapid transition, 116
VLAN port link type, 171
voice VLAN port operation configuration (automatic assignment), 219
voice VLAN port operation configuration (manual assignment), 220
voice VLAN port operation mode, 217
port isolation
configuration, 94
collection (multiple isolation groups), 95
display, 94
group assignment (multiple ports), 94
port speed
Ethernet link aggregation member port state, 63
port-based VLAN
assignment (access port), 173
assignment (hybrid port), 174
assignment (trunk port), 173
configuration, 171, 183
port frame handling, 172
port link type, 171
PVID, 172
priority
DR role, 336
DR role priority, 343
DR system priority, 343
dynamic link aggregation, 50
Ethernet link aggregation LACP, 50
Ethernet link aggregation LACP port priority, 50
Ethernet link aggregation LACP system priority, 50
LLDP 802.1p-to-local priority mapping, 307
LLDP PFC 802.1p priority, 309
MAC address table learning priority, 34
priority-based flow control. Use PFC
QinQ SVLAN tag 802.1p priority, 249
spanning tree device priority, 124
spanning tree port priority configuration, 132
private VLAN
configuration, 197, 198, 200
configuration restrictions, 198
display, 200
promiscuous port configuration, 200
secondary VLAN Layer 3 communication configuration, 210
trunk promiscuous port configuration, 203
trunk promiscuous+secondary port configuration, 206
procedure
adding MAC address table blackhole entry, 30
adding MAC address table entry (global), 29
adding MAC address table entry (on interface), 30
adding MAC address table multiport unicast entry, 31
assigning aggregate interface to DR group, 346
assigning MAC address table learning priority to interface, 34
assigning port isolation group (multiple ports), 94
assigning port-based VLAN access port (interface view), 173
assigning port-based VLAN access port (VLAN view), 173
assigning port-based VLAN hybrid port, 174
assigning port-based VLAN trunk port, 173
bulk configuring interfaces, 25, 25
changing Ethernet aggregate interface (MAC address), 62
changing Ethernet interface to FC interface (Layer 2), 16
combining Ethernet interfaces (10-GE > 40-GE), 2
configuring 1:1 VLAN mapping, 261, 267
configuring 1:2 VLAN mapping, 266, 273
configuring 2:2 VLAN mapping, 267, 273
configuring common Ethernet interface settings, 2
configuring DR keepalive packet parameters, 345
configuring DR keepalive settings, 344
configuring DR system auto-recovery, 349
configuring DR system MAC, 342
configuring DR system number, 342
configuring DR system priority, 343
configuring DR system settings, 342
configuring DRNI, 341
configuring DRNI with PVST, 157
configuring Ethernet aggregate interface, 61
configuring Ethernet aggregate interface (description), 61
configuring Ethernet interface (Layer 2), 15
configuring Ethernet interface (Layer 3), 20
configuring Ethernet interface basic settings, 4
configuring Ethernet interface dampening, 7
configuring Ethernet interface generic flow control, 10
configuring Ethernet interface jumbo frame support, 6
configuring Ethernet interface link mode, 5
configuring Ethernet interface PFC, 11
configuring Ethernet interface physical state change suppression, 6
configuring Ethernet interface storm control (Layer 2), 15
configuring Ethernet interface storm suppression, 14
configuring Ethernet link aggregate interface (Layer 2 edge), 85
configuring Ethernet link aggregation, 55
configuring Ethernet link aggregation (Layer 2 dynamic), 80
configuring Ethernet link aggregation (Layer 2 static), 79
configuring Ethernet link aggregation (Layer 3 dynamic), 87
configuring Ethernet link aggregation (Layer 3 static), 86
configuring Ethernet link aggregation edge aggregate interface, 65
configuring Ethernet link aggregation group, 56
configuring Ethernet link aggregation group (Layer 2 dynamic), 57
configuring Ethernet link aggregation group (Layer 2 static), 57
configuring Ethernet link aggregation group (Layer 3 dynamic), 59
configuring Ethernet link aggregation group (Layer 3 static), 58
configuring Ethernet link aggregation group BFD, 66
configuring Ethernet link aggregation group load sharing, 69
configuring Ethernet link aggregation load sharing (Layer 2), 82
configuring Ethernet link aggregation load sharing (Layer 3), 89
configuring Ethernet link aggregation load sharing algorithm settings, 72
configuring Ethernet subinterface (Layer 3), 20
configuring Ethernet subinterface basic settings, 4
configuring interface (inloopback), 24
configuring interface (loopback), 23
configuring interface (null), 23
configuring IP subnet-based VLAN, 180, 187
configuring L2PT, 325
configuring L2PT for LACP, 328
configuring L2PT for STP, 327
configuring LAN switching QinQ VLAN tag TPID value, 248
configuring Layer 2 forwarding (cut-through), 334
configuring LLDP, 292
configuring LLDP (CDP-compatible), 316
configuring LLDP 802.1p-to-local priority mapping, 307
configuring LLDP advertiseable TLVs, 295
configuring LLDP APP parameters, 305
configuring LLDP basics, 293, 312
configuring LLDP CDP compatibility, 301
configuring LLDP DCBX, 303, 317
configuring LLDP DCBX version, 305
configuring LLDP ETS parameters, 307
configuring LLDP group-based WRR queuing, 308
configuring LLDP management address, 298
configuring LLDP management address encoding format, 298
configuring LLDP neighbor aging, 303
configuring LLDP neighbor validation, 302
configuring LLDP neighbor validation and aging, 302
configuring LLDP PFC parameters, 309
configuring LLDP trapping, 309
configuring LLDP-MED trapping, 309
configuring loop detection, 162, 164
configuring M:1 VLAN mapping, 261, 267
configuring M:1 VLAN mapping (dynamic IP address assignment), 261
configuring M:1 VLAN mapping (static IP address assignment), 264
configuring M:1 VLAN mapping customer-side port (dynamic IP address assignment), 262
configuring M:1 VLAN mapping customer-side port (static IP address assignment), 264
configuring M:1 VLAN mapping network-side port (dynamic IP address assignment), 263
configuring M:1 VLAN mapping network-side port (static IP address assignment), 265
configuring MAC address move suppression, 37
configuring MAC address table, 28, 40
configuring MAC address table frame forwarding rule, 34
configuring MAC address table multiport unicast entry (global), 31
configuring MAC address table multiport unicast entry (on interface), 31
configuring MAC Information, 43
configuring MAC Information mode, 42
configuring MAC-based VLAN, 175, 185
configuring MAC-based VLAN (server-assigned), 180
configuring MAC-based VLAN assignment (dynamic), 178
configuring MAC-based VLAN assignment (static), 178
configuring management Ethernet interface, 1
configuring MST region, 122
configuring MST region max hops, 124
configuring MSTP, 121, 150
configuring MVRP, 231, 234
configuring PBB, 280, 283
configuring PBB data encapsulation type, 282, 282
configuring PBB downlink port, 281
configuring PBB uplink port, 281
configuring PBB VSI B-VLAN, 281
configuring port isolation (multiple isolation groups), 95
configuring port-based VLAN, 171, 183
configuring private VLAN, 197, 198
configuring private VLAN promiscuous port, 200
configuring private VLAN trunk promiscuous port, 203
configuring private VLAN trunk promiscuous+secondary port, 206
configuring protocol-based VLAN, 181, 188
configuring PVST, 120, 154
configuring QinQ basics, 251
configuring QinQ CVLAN tag TPID value, 249
configuring QinQ SVLAN tag TPID value, 249
configuring QinQ VLAN transparent transmission, 247, 253
configuring RSTP, 119
configuring S-channel bundle group (dynamic), 60
configuring S-channel bundle group (static), 60
configuring secondary VLAN Layer 3 communication, 210
configuring service loopback group, 332, 333
configuring simple multichassis link aggregation (S-MLAG), 77
configuring S-MLAG (Layer 2 dynamic), 91
configuring spanning tree, 118
configuring spanning tree BPDU guard, 142
configuring spanning tree BPDU transmission rate, 127
configuring spanning tree device priority, 124
configuring spanning tree Digest Snooping, 136, 137
configuring spanning tree edge port, 128
configuring spanning tree No Agreement Check, 138, 140
configuring spanning tree port link type, 132
configuring spanning tree port mode for MSTP frames, 133
configuring spanning tree port path cost, 128, 131
configuring spanning tree port priority, 132
configuring spanning tree port role restriction, 144
configuring spanning tree protection, 142
configuring spanning tree root bridge, 123
configuring spanning tree root bridge (device), 123
configuring spanning tree secondary root bridge, 123
configuring spanning tree secondary root bridge (device), 124
configuring spanning tree switched network diameter, 125
configuring spanning tree TC Snooping, 140
configuring spanning tree TC-BPDU transmission restriction, 144
configuring spanning tree timeout factor, 127
configuring spanning tree timer, 125
configuring STP, 118
configuring super VLAN, 192, 192, 194
configuring super VLAN interface, 193
configuring VLAN basic settings, 169
configuring VLAN group, 182
configuring VLAN interface, 170
configuring VLAN mapping, 260
configuring voice VLAN, 218
configuring voice VLAN advertisement (CDP), 222
configuring voice VLAN advertisement (LLDP), 222
configuring voice VLAN assignment mode (automatic), 223
configuring voice VLAN assignment mode (manual), 225
configuring voice VLAN port operation (automatic assignment), 219
configuring voice VLAN port operation (manual assignment), 220
configuring voice VLAN traffic QoS priority settings, 218
creating PBB VSI, 280
creating super VLAN sub-VLAN, 192
disabling DRNI configuration consistency check, 347
disabling LLDP PVID inconsistency check, 300
disabling MAC address learning (global), 32
disabling MAC address learning (on interface), 32
disabling MAC address learning (on VLAN), 33
disabling MAC address table static source check, 38
disabling spanning tree dispute guard, 146
disabling spanning tree inconsistent PVID protection, 136
disabling the device to reactivate the shutdown edge ports, 148
displaying bulk interface configuration, 26
displaying DRNI, 350
displaying Ethernet interface, 21
displaying Ethernet link aggregation, 78
displaying Ethernet subinterface, 21
displaying interface, 24
displaying L2PT, 326
displaying LLDP, 311
displaying loop detection, 164
displaying MAC address table, 40
displaying MVRP, 234
displaying PBB, 283
displaying port isolation, 94
displaying private VLAN, 200
displaying QinQ, 250
displaying service loopback group, 333
displaying spanning tree, 149
displaying super VLAN, 193
displaying VLAN, 183
displaying VLAN mapping, 267
displaying VLAN mapping, 267
displaying voice VLAN, 223
enable Ethernet interface bridging (Layer 2), 19
enabling Ethernet interface link flapping protection, 8
enabling Ethernet interface loopback testing, 9
enabling Ethernet link aggregation local-first load sharing, 71
enabling Ethernet link aggregation traffic redirection, 72
enabling Ethernet subinterface packet statistics, 21
enabling L2PT, 325
enabling L2PT (for protocol), 325
enabling Layer 3 aggregate subinterface packet statistics, 68
enabling LLDP, 293
enabling LLDP ARP entry generation, 311
enabling LLDP polling, 295
enabling LLDP+DCBX TLV advertisement, 304
enabling loop detection (global), 162
enabling loop detection (port-specific), 162
enabling M:1 VLAN mapping ARP detection (dynamic IP address assignment), 262
enabling M:1 VLAN mapping ARP snooping (static IP address assignment), 264
enabling M:1 VLAN mapping DHCP snooping (dynamic IP address assignment), 262
enabling MAC address synchronization, 35
enabling MAC address table ARP fast update, 38
enabling MAC address table move notification, 37
enabling MAC address table SNMP notification, 39
enabling MAC Information, 42
enabling MVRP, 232
enabling MVRP GVRP compatibility, 234
enabling PBB L2VPN, 280
enabling port bridging on Layer 2 aggregate interface, 75
enabling PVST BPDU guard, 146
enabling QinQ, 247
enabling remote fault signal detection, 15
enabling short DRCP timeout timer, 348
enabling spanning tree BPDU drop, 145
enabling spanning tree BPDU guard (global), 142
enabling spanning tree BPDU guard (on interface), 142
enabling spanning tree BPDU transparent transmission (on port), 148
enabling spanning tree feature, 134
enabling spanning tree loop guard, 143
enabling spanning tree port state transition information output, 133
enabling spanning tree root guard, 143
enabling spanning tree SNMP notification (new-root election, topology change events), 149
enabling spanning tree TC BPDU event logging (PVST mode), 148
enabling spanning tree TC-BPDU guard, 145
enabling transparent LACPDU transmission, 76
enabling voice VLAN LLDP automatic IP phone discovery, 221
excluding interface from shutdown action by DRNI MAD (F2611 and later), 344
excluding interface from shutdown action by DRNI MAD (Release 2609), 344
forcing Ethernet interface fiber port (Layer 2), 17
ignoring Ethernet link aggregation member port state (port speed), 63
maintaining DRNI, 350
maintaining Ethernet interface, 21
maintaining Ethernet link aggregation, 78
maintaining Ethernet subinterface, 21
maintaining interface, 24
maintaining L2PT, 326
maintaining MVRP, 234
maintaining PBB, 283
maintaining spanning tree, 149
maintaining VLAN, 183
modifying MAC address table blackhole entry, 30
modifying MAC address table entry (global), 29
modifying MAC address table entry (on interface), 30
modifying MAC address table multiport unicast entry, 31
performing spanning tree mCheck, 135
performing spanning tree mCheck globally, 135
performing spanning tree mCheck in interface view, 136
restoring Ethernet link aggregate interface default settings, 69
setting data restoration interval, 349
setting DR role priority, 343
setting Ethernet interface connection distance (Layer 2), 20
setting Ethernet interface MAC address (Layer 2), 20
setting Ethernet interface MDIX mode (Layer 2), 18
setting Ethernet interface MTU (Layer 3), 20
setting Ethernet interface statistics polling interval, 13
setting Ethernet link aggregate group Selected ports min/max, 64
setting Ethernet link aggregate interface (expected bandwidth), 65
setting Ethernet link aggregation load sharing mode (global), 70
setting Ethernet link aggregation load sharing mode (group-specific), 70
setting Ethernet link aggregation load sharing mode for MAC-in-MAC traffic (global), 72
setting Ethernet subinterface MAC address (Layer 3), 20
setting Ethernet subinterface MTU (Layer 3), 20
setting keepalive hold timer, 348
setting keepalive interval, 346
setting keepalive timeout timer, 346
setting L2PT tunneled packet destination multicast MAC address, 326
setting Layer 3 aggregate interface (MTU), 63
setting LLDP bridge mode, 293
setting LLDP frame encapsulation format, 300
setting LLDP operating mode, 294
setting LLDP parameters, 299
setting LLDP reinitialization delay, 294
setting LLDP source MAC address, 310
setting loop detection interval, 164
setting loop detection protection action (global), 163
setting loop detection protection action (Layer 2 aggregate interface), 163
setting loop detection protection action (Layer 2 Ethernet interface), 163
setting loop detection protection action (S-channel aggregate interface), 163
setting loop detection protection action (S-channel bundle interface), 163
setting loop detection protection action (S-channel interface), 163
setting MAC address table dynamic aging timer, 33
setting MAC address table learning limit, 34
setting MAC Information change notification interval, 43
setting MAC Information queue length, 43
setting MVRP registration mode, 232
setting MVRP timer, 233
setting PFC thresholds, 12
setting QinQ SVLAN tag 802.1p priority, 249
setting spanning tree mode, 121
shutting down Ethernet link aggregate interface, 68
specifying default link-aggregation load sharing ignored packet fields, 70
specifying IPP, 347
specifying Layer 2 aggregate interface (ignored VLAN), 62
specifying link aggregation management subnet, 74, 74
specifying link aggregation management VLAN+management port, 74, 74
specifying spanning tree port path cost calculation standard, 128
splitting Ethernet interface (40-GE), 2
testing Ethernet interface cable connection (Layer 2), 19
troubleshooting PBB customer frames cannot be transmitted, 285

promiscuous
private VLAN promiscuous port configuration, 200
private VLAN trunk promiscuous port configuration, 203
private VLAN trunk promiscuous+secondary port configuration, 206

protecting
disabling the device to reactivate the shutdown edge ports, 148
loop detection protection action setting, 163
spanning tree protection, 142
spanning tree SNMP notification (new-root election, topology change events), 149

protocol-based VLAN
configuration, 181, 188

protocols and standards
DRNI, 341
Ethernet link aggregation protocol configuration, 47
LLDP, 292
MSTP, 117
MSTP protocol frames, 109
MVRP, 231
PBB, 279
PVST protocol frames, 108
QinQ, 247
RSTP protocol frames, 106
STP protocol frames, 97
VLAN, 169

provider
backbone bridge. Use PBB backbone bridge network. See PBBN backbone network. See PBN

PVID
spanning tree inconsistent PVID protection disable, 136
PVID (port-based VLAN), 172
PVST, 97, See also STP
basic concepts, 109
configuration, 120, 154
feature enable, 134
how it works, 109
mode set, 121
port links, 108
protocol frames, 108
rapid transition, 115
spanning tree TC BPDU event logging (PVST mode), 148

Q

QinQ
basic configuration, 251
configuration, 245, 251
configuration restrictions, 247
CVLAN tag, 245
display, 250
enable, 247
how it works, 245
implementation, 246
loop detection configuration, 160, 162, 164
protocols and standards, 247
SVLAN tag, 245
SVLAN tag 802.1p priority, 249
VLAN tag TPID value, 248
VLAN transparent transmission, 247
VLAN transparent transmission configuration, 253

QoS
- LLDP 802.1p-to-local priority mapping, 307
- LLDP APP parameters, 305
- LLDP DCBX version, 305
- LLDP ETS parameters, 307
- LLDP group-based WRR queuing, 308
- LLDP PFC parameters, 309
- QinQ SVLAN tag 802.1p priority, 249
- voice VLAN traffic QoS priority settings, 218
- queuing
  - MAC Information queue length, 43

Rapid Spanning Tree Protocol. Use RSTP rate
- spanning tree BPDU transmission rate, 127
- receiving
  - LLDP frames, 292
- recovering
  - loop detection port status auto recovery, 161
- redirecting
  - Ethernet link aggregation traffic redirection, 72
- reference port (Ethernet link aggregation), 48, 52
- reference port speed (Ethernet link aggregation), 67
- region
  - MST, 112
  - MST region configuration, 122
  - MST region max hops, 124
  - MST regional root, 112
- registering
  - MVRP registration fixed mode, 231
  - MVRP registration forbidden mode, 231
  - MVRP registration mode, 232
  - MVRP registration normal mode, 231
- reinitialization delay (LLDP), 294
- restoring
  - Ethernet link aggregate interface default settings, 69
- restrictions
  - bulk interface configuration, 25
  - DRNI restrictions, 341
  - Ethernet interface dampening, 8
  - Ethernet interface link flapping protection, 9
  - Ethernet interface loopback test, 9
  - Ethernet interface PFC configuration, 11
  - Ethernet interface storm suppression, 14
  - Ethernet link aggregation BFD configuration, 66
  - Ethernet link aggregation group, 56
  - Ethernet link aggregation traffic redirection, 73
  - L2PT enable, 325
  - Layer 2 Ethernet interface fiber port, 18
  - Layer 2 Ethernet interface storm control configuration, 16
  - LLDP APP parameter configuration, 306
  - M:1 VLAN mapping configuration (dynamic IP address assignment), 261
  - M:1 VLAN mapping configuration (static IP address assignment), 264
  - MAC Information configuration, 44
  - MAC-based VLAN assignment configuration (dynamic), 178
  - MVRP configuration, 231
  - PBB configuration, 280
  - private VLAN configuration, 198
  - QinQ configuration, 247
  - spanning tree port role restriction, 144
  - spanning tree TC-BPDU transmission restriction, 144
- STP Digest Snooping configuration, 137
- STP edge port configuration, 128
- STP mCheck configuration, 135
- STP port link type configuration, 132
- STP TC Snooping configuration, 141
- STP timer configuration, 126
- VLAN configuration, 178
- voice VLAN LLDP automatic IP phone discovery enable, 221
- voice VLAN port operation configuration (automatic assignment), 219
- voice VLAN port operation configuration restrictions (manual assignment), 220
- role
  - DR member device role, 336
  - DR role priority, 343
  - DR system auto-recovery, 349
- root
  - MST common root bridge, 113
  - MST regional root, 112
  - MST root port role, 113
  - spanning tree root bridge, 123
  - spanning tree root bridge (device), 123
  - spanning tree root guard, 143
  - spanning tree secondary root bridge (device), 124
  - STP algorithm calculation, 100
  - STP edge port rapid transition, 116
  - STP root bridge, 99
  - STP root port, 99
- routing
IP subnet-based VLAN configuration, 180, 187
MAC-based VLAN assignment (dynamic), 178
MAC-based VLAN assignment (static), 178
MAC-based VLAN configuration, 175, 185
MAC-based VLAN configuration (server-assigned), 180
protocol-based VLAN configuration, 181, 188
voice VLAN configuration, 213, 218, 223
voice VLAN IP phone access method, 214

RSTP, 97, See also STP
basic concepts, 106
BPDU processing, 107
configuration, 119
feature enable, 134
how it works, 107
mode set, 121
MSTP device implementation, 115
network convergence, 106
port role, 106
port state, 106
protocol frames, 106
rapid transition, 115

rule
MAC address table frame forwarding rule, 34

S
S-channel
bundle group (dynamic), 60
bundle group (static), 60
bundle group configuration, 60

security
voice VLAN operation mode, 217

selecting
Ethernet link aggregation reference port, 67
Ethernet link aggregation Selected ports min/max, 64
Ethernet link aggregation selected state, 47
Ethernet link aggregation unselected state, 47

series
voice VLAN host+IP phone connection (in series), 214

server
MAC-based VLAN assignment (server-assigned), 177
MAC-based VLAN configuration (server-assigned), 180

service
LLDP service bridge mode, 293
service loopback group configuration, 332, 333
display, 333

setting
data restoration interval, 349
DR role priority, 343
DR system auto-recovery, 349
Ethernet interface connection distance (Layer 2), 20
Ethernet interface MAC address (Layer 3), 20
Ethernet interface MDIX mode (Layer 2), 18
Ethernet interface MTU (Layer 3), 20
Ethernet interface PFC thresholds, 12
Ethernet interface statistics polling interval, 13
Ethernet link aggregate group Selected ports min/max, 64
Ethernet link aggregate interface (expected bandwidth), 65
Ethernet link aggregation load sharing mode (global), 70
Ethernet link aggregation load sharing mode (group-specific), 70
Ethernet link aggregation load sharing mode for MAC-in-MAC traffic (global), 72
Ethernet link aggregation member port state, 49, 53
Ethernet subinterface MAC address (Layer 3), 20
Ethernet subinterface MTU (Layer 3), 20
keepalive hold timer, 348
keepalive interval, 346
keepalive timeout timer, 346
L2PT tunneled packet destination multicast MAC address, 326
Layer 3 aggregate interface (MTU), 63
LLDP bridge mode, 293
LLDP frame encapsulation format, 300
LLDP operating mode, 294
LLDP parameters, 299
LLDP reinitialization delay, 294
LLDP source MAC address, 310
loop detection interval, 164
loop detection protection action (global), 163
loop detection protection action (Layer 2 aggregate interface), 163
loop detection protection action (Layer 2 Ethernet interface), 163
loop detection protection action (S-channel aggregate interface), 163
loop detection protection action (S-channel bundle interface), 163
loop detection protection action (S-channel interface), 163
MAC address table dynamic aging timer, 33
MAC address table learning limit, 34
MAC Information change notification interval, 43
MAC Information queue length, 43
MVRP registration mode, 232
MVRP timer, 233
QinQ SVLAN tag 802.1p priority, 249
spanning tree mode, 121
shutting down
  Ethernet link aggregate interface, 68
  loop detection shutdown action, 161
SNAP
  LLDP frame encapsulation, 287
  LLDP frame encapsulation format, 300
SNMP
  MAC address table SNMP notification, 39
  MAC Information configuration, 42, 43
snooping
  spanning tree Digest Snooping, 136, 137
  spanning tree TC Snooping, 140
source
  MAC address table static source check, 38
spanning tree, 97, See also STP, RSTP, PVST, MSTP
  BPDU drop, 145
  BPDU guard configuration, 142
  BPDU transmission rate configuration, 127
  BPDU transparent transmission (on port), 148
  configuration, 97, 118, 150
  device priority configuration, 124
  Digest Snooping, 136, 137
  disabling the device to reactivate the shutdown edge ports, 148
  display, 149
  dispute guard disable, 146
  edge port configuration, 128
  feature enable, 134
  inconsistent PVID protection disable, 136
  loop guard enable, 143
  maintain, 149
  mCheck, 135
  mode set, 121
  MST region max hops, 124
  No Agreement Check, 138, 140
  port link type configuration, 132
  port mode configuration, 133
  port path cost calculation standard, 128
  port path cost configuration, 128, 131
  port priority configuration, 132
  port role restriction, 144
  port state transition output, 133
  protection configuration, 142
  PVST BPDU guard, 146
  root bridge configuration, 123
  root bridge configuration (device), 123
  root guard enable, 143
  secondary root bridge configuration (device), 124
SNMP notification enable (new-root election, topology change events), 149
switched network diameter, 125
TC BPDU event logging (PVST mode), 148
TC Snooping, 140
TC-BPDU guard, 145
TC-BPDU transmission restriction, 144
timeout factor configuration, 127
timer configuration, 125
specifying
  IPP, 347
  Layer 2 aggregate interface (ignored VLAN), 62
  link aggregation management subnet, 74
  link aggregation management VLAN+management port, 74
  spanning tree port path cost calculation standard, 128
splitting
  Ethernet interface (40-GE), 2
state
  Ethernet interface state change suppression, 6
  Ethernet link aggregation member port state, 47, 49, 53
static
  Ethernet link aggregation (Layer 2), 79
  Ethernet link aggregation (Layer 3), 86
  Ethernet link aggregation (static mode), 48
  Ethernet link aggregation group, 57, 58
  Ethernet link aggregation group BFD, 66
  Ethernet link aggregation mode, 48
  Layer 2 Ethernet link aggregation group, 57
  Layer 3 Ethernet link aggregation group, 58
  MAC address table entry, 27
  MAC address table entry configuration (global), 29
  MAC address table entry configuration (on interface), 30
  MAC address table static source check, 38
  MAC-based VLAN assignment, 175, 178
  S-channel bundle group, 60
statistics
  Ethernet interface statistics polling interval, 13
  Ethernet subinterface packet statistics, 21
storm
  Ethernet interface storm control (Layer 2), 15
  Ethernet interface storm suppression, 14
STP
  algorithm calculation, 100
basic concepts, 99
BPDU forwarding, 105
configuration, 118
configuration BPDUs, 97
designated bridge, 99
designated port, 99
Digest Snooping configuration restrictions, 137
designated port configuration restrictions, 128
edge port configuration restrictions, 128
feature enable, 134
L2PT for STP configuration, 327
loop detection, 97
mCheck configuration restrictions, 135
mode set, 121
MSTP device implementation, 115
P/A transition, 116
path cost, 100
port link type configuration restrictions, 132
port state, 99
protocol frames, 97
root bridge, 99
root port, 99
TC Snooping configuration restrictions, 141
TCN BPDUs, 98
timer configuration restrictions, 126
 timers, 105
subinterface, 1, See also Ethernet subinterface
 LLDP ARP entry generation, 311
 LLDP source MAC address, 310
 subnetting
 IP subnet-based VLAN configuration, 180, 187
 sub-VLAN
 creation, 192
 super VLAN
 configuration, 192, 192, 194
 display, 193
 interface configuration, 193
 sub-VLAN creation, 192
 suppressing
 Ethernet interface physical state change, 6
 Ethernet interface storm, 14
 Ethernet interface storm control configuration (Layer 2), 15
 MAC address move, 37
SVLAN
 QinQ basic configuration, 251
 QinQ configuration, 245, 251
 QinQ SVLAN tag 802.1p priority, 249
 QinQ VLAN transparent transmission configuration, 253
VLAN mapping application scenario, 255
VLAN mapping configuration, 255, 260, 267
VLAN mapping implementation, 257
switching
 Ethernet interface configuration, 1
 interface configuration (inloopback), 23, 24
 interface configuration (loopback), 23, 23
 interface configuration (null), 23, 23
 spanning tree switched network diameter, 125
synchronizing
 MAC addresses, 35
 syslog
 MAC Information configuration, 42, 43
 MAC Information mode configuration, 42
 system
 configuration consistency check, 338
 disabling configuration consistency check, 347
 DR system MAC, 342
 DR system number, 342
 DR system priority, 343
 DR system settings, 342
 DR system setup, 337
 interface bulk configuration, 25, 25
 MAD mechanism, 337
T
 table
 LLDP priority mapping table, 307
 MAC address, 27, 28, 40
 MAC address table learning limit, 34
 MSTP VLAN-to-instance mapping table, 112
 tag
 1:1 VLAN mapping configuration, 261, 267
 1:2 VLAN mapping configuration, 266, 273
 2:2 VLAN mapping configuration, 267, 273
 M:1 VLAN mapping configuration, 261, 267
 M:1 VLAN mapping configuration (dynamic IP address assignment), 261
 M:1 VLAN mapping configuration (static IP address assignment), 264
 QinQ CVLAN, 245
 QinQ SVLAN, 245
 QinQ SVLAN tag 802.1p priority, 249
 QinQ VLAN tag TPID value, 248
 VLAN mapping configuration, 255, 260, 267
 TC Snooping (spanning tree), 140
 TC-BPDU
 spanning tree TC-BPDU guard, 145
 spanning tree TC-BPDU transmission restriction, 144
 testing
Ethernet interface cable connection (Layer 2),

- 19 time

- Ethernet link aggregation LACP timeout interval, 50

- Ethernet link aggregation LACP long timeout interval, 51

- Ethernet link aggregation LACP short timeout interval, 51

- short DRCP timeout timer, 348

- spanning tree timeout factor, 127

- timer

- DR keepalive timeout timer, 346

- DRCP timeout timers, 336

- keepalive hold timer, 348

- LLDP reinitialization delay, 294

- MAC address table dynamic aging, 33

- MRP Join, 230

- MRP Leave, 230

- MRP LeaveAll, 230

- MRP Periodic, 230

- MVRP set, 233

- short DRCP timeout timer, 348

- spanning tree forward delay, 125

- spanning tree hello, 125

- spanning tree max age, 125

- STP forward delay, 105

- STP hello, 105

- STP max age, 105

- TLV

- LLDP advertisable TLV configuration, 295

- LLDP management address configuration, 298

- LLDP management address encoding format, 298

- LLDP parameters, 299

- LLDP+DCBX TLV advertisement, 304

- LLDPDU basic management types, 288

- LLDPDU LLDP-MED types, 288

- LLDPDU management address TLV, 291

- LLDPDU organization-specific types, 288

- topology

- PVST BPDU protocol frames, 108

- STP TCN BPDU protocol frames, 97

- traffic

- Ethernet link aggregation traffic redirection, 72

- PBB configuration, 276, 280, 283

- private VLAN configuration, 198, 200

- voice VLAN traffic QoS priority settings, 218

- transmitting

- LLDP frames, 291

- QinQ VLAN transparent transmission, 247, 253

- spanning tree TC-BPDU transmission restriction, 144

- transparent transmission (QinQ for VLAN), 247, 253

- trapping

- LLDP configuration, 309

- LLDP-MED configuration, 309

- MAC Information configuration, 42, 43

- MAC Information mode configuration, 42

- troubleshooting

- PBB, 285

- PBB customer frames cannot be transmitted, 285

- trunk port

- port-based VLAN assignment (trunk port), 173

- private VLAN trunk promiscuous port configuration, 203

- private VLAN trunk promiscuous+secondary port configuration, 206

- tunneling

- L2PT configuration, 323, 325, 327

- L2PT enable, 325

- L2PT for LACP configuration, 328

- L2PT for STP configuration, 327

- L2PT tunneled packet destination multicast MAC address, 326

- U

- unicast

- MAC address table configuration, 27, 28, 40

- MAC address table multiport unicast entry, 27

- uplink

- PBB port configuration, 281

- V

- virtual

- Virtual Local Area Network. Use VLAN

- virtualization

- distributed relay, 335, 350, 350

- Distributed Resilient Network Interconnect, 335, 350

- VLAN

- basic configuration, 169

- configuration, 168, 183

- configuration restrictions, 178

- display, 183

- frame encapsulation, 168

- group configuration, 182

- interface configuration, 170

- IP subnet-based VLAN configuration, 180, 187
L2PT configuration, 323, 325, 327
L2PT for LACP configuration, 328
L2PT for STP configuration, 327
Layer 2 Ethernet aggregate interface (ignored VLAN), 62
link aggregation management subnet, 74
link aggregation management VLAN+management port, 74
LLDP CDP compatibility, 301
LLDP configuration (CDP-compatible), 316
LLDP source MAC address, 310
loop detection configuration, 160, 162, 164
MAC address learning disable, 33
MAC-based assignment (dynamic), 178
MAC-based assignment (static), 178
MAC-based configuration, 185
MAC-based VLAN configuration, 175
MAC-based VLAN configuration (server-assigned), 180
maintain, 183
mapping. See VLAN mapping
MRP implementation, 228
MSTP VLAN-to-instance mapping table, 112
MVRP configuration, 228, 231, 234
MVRP GVRP compatibility, 234
PBB data encapsulation type, 282
port isolation configuration, 94
port link type, 171
port-based configuration, 171, 183
port-based VLAN assignment (access port), 173
port-based VLAN assignment (hybrid port), 174
port-based VLAN assignment (trunk port), 173
port-based VLAN frame handling, 172
private VLAN configuration, 197, 198
private VLAN configuration restrictions, 198
protocol-based VLAN configuration, 181, 188
protocols and standards, 169
PVID, 172
PVST, 108
QinQ basic configuration, 251
QinQ configuration, 245, 251
QinQ CVLAN tag, 245
QinQ implementation, 246
QinQ SVLAN tag, 245
QinQ SVLAN tag 802.1p priority, 249
QinQ transparent transmission, 247
QinQ VLAN tag TPID value, 248
QinQ VLAN transparent transmission configuration, 253
spanning tree inconsistent PVID protection disable, 136
super VLAN configuration, 192, 192, 194
super VLAN interface configuration, 193
termination. See VLAN termination
voice VLAN advertisement (CDP), 222
voice VLAN advertisement (LLDP), 222
voice VLAN assignment mode, 215
voice VLAN assignment mode configuration (automatic), 223
voice VLAN assignment mode configuration (manual), 225
voice VLAN configuration, 213, 218, 223
voice VLAN host+IP phone connection (in series), 214
voice VLAN IP phone access method, 214
voice VLAN IP phone+device connection, 215
voice VLAN LLDP automatic IP phone discovery enable, 221
voice VLAN port operation configuration (automatic assignment), 219
voice VLAN port operation configuration (manual assignment), 220
voice VLAN port operation configuration restrictions (automatic assignment), 219
voice VLAN port operation configuration restrictions (manual assignment), 220
voice VLAN port operation mode, 217
voice VLAN traffic QoS priority settings, 218
VLAN mapping
0:2 application scenario, 255
0:2 implementation, 257
1:1 application scenario, 255, 255
1:1 configuration, 261, 267
1:1 implementation, 257, 258
1:2 application scenario, 255, 256
1:2 configuration, 266, 273
1:2 implementation, 257, 259
2:2 application scenario, 255, 256
2:2 configuration, 267, 273
2:2 implementation, 257, 259
2:3 application scenario, 255
2:3 implementation, 257
configuration, 255, 260, 267
display, 267
M:1 application scenario, 255, 255
M:1 configuration, 261, 267
M:1 configuration (dynamic IP address assignment), 261
M:1 configuration (static IP address assignment), 264
M:1 implementation, 257, 258
voice traffic
   LLDP CDP compatibility, 301
   LLDP configuration (CDP-compatible), 316

voice VLAN
   advertisement configuration (CDP), 222
   advertisement configuration (LLDP), 222
   assignment mode, 215
   assignment mode (automatic), 215
   assignment mode (manual), 216
   assignment mode configuration (automatic), 223
   assignment mode configuration (manual), 225
   assignment mode+IP phone cooperation, 216
   configuration, 213, 218, 223
   display, 223
   host+IP phone connection (in series), 214
   information advertisement to IP phone, 214
   IP phone access method, 214
   IP phone identification (LLDP), 214
   IP phone identification (OUI address), 213
   IP phone identification method, 213
   IP phone+device connection, 215
   LLDP automatic IP phone discovery enable, 221
   LLDP automatic IP phone discovery enable restrictions, 221
   port operation configuration (automatic assignment), 219
   port operation configuration (manual assignment), 220
   port operation configuration restrictions (automatic assignment), 219
   port operation configuration restrictions (manual assignment), 220
   port operation mode, 217
   traffic QoS priority setting configuration, 218

VoIP
   voice VLAN configuration, 213, 218, 223
   voice VLAN information advertisement to IP phones, 214
   voice VLAN IP phone access method, 214
   voice VLAN IP phone identification (LLDP), 214
   voice VLAN IP phone identification (OUI address), 213

VPLS
   transparent LACPDU transmission, 76

VPN
   PBB configuration, 276, 280, 283
   QinQ basic configuration, 251
   QinQ configuration, 245, 251

QinQ VLAN transparent transmission configuration, 253

VSI
   PBB B-VLAN configuration, 281
   PBB creation, 280

W
   WRR queuing
      LLDP group-based WRR queuing, 308