Copyright © 2011-2012, Hangzhou H3C Technologies Co., Ltd. and its licensors

All rights reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Hangzhou H3C Technologies Co., Ltd.

Trademarks

H3C, H3C, Aolynk, H3Care, TOP G, IRF, NetPilot, Neoc1an, NeovTL, SecPro, SecPoint, SecEngine, SecPath, Comware, Secware, Storware, NQA, VVG, V^G, V^G, PSPT, XGbus, N-Bus, TiGem, InnoVision and HUASAN are trademarks of Hangzhou H3C Technologies Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.
The H3C SR8800 documentation set includes 13 configuration guides, which describe the software features for the H3C SR8800 10G Core Routers and guide you through the software configuration procedures. These configuration guides also provide configuration examples to help you apply software features to different network scenarios.

The Layer 2—LAN Switching Configuration Guide describes the fundamentals and configuration of Ethernet link aggregation, port isolation, spanning tree, VLAN, and so on. It describes how you can use these technologies to isolate users in the same VLAN, eliminate Layer 2 loops, divide VLANs, transmit customer network packets through the service provider network, modify the VLAN tags of packets, and so on.

This preface includes:
- Audience
- Conventions
- About the H3C SR8800 documentation set
- Obtaining documentation
- Technical support
- Documentation feedback

**Audience**

This documentation is intended for:
- Network planners
- Field technical support and servicing engineers
- Network administrators working with the SR8800 series

**Conventions**

This section describes the conventions used in this documentation set.

**Command conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td><strong>Bold</strong> 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>
</tbody>
</table>
### Convention Description

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 <strong>New User</strong> window appears; click <strong>OK</strong>.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, <strong>File &gt; Create &gt; Folder</strong>.</td>
</tr>
</tbody>
</table>

#### Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️ <strong>WARNING</strong></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>△ <strong>CAUTION</strong></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>🔴 <strong>IMPORTANT</strong></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>💡 <strong>TIP</strong></td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>

#### Network topology icons

- Represents a generic network device, such as a router, switch, or firewall.
- Represents a routing-capable device, such as a router or Layer 3 switch.
- Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.

#### Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your router.

### About the H3C SR8800 documentation set

The H3C SR8800 documentation set includes:

<table>
<thead>
<tr>
<th>Category</th>
<th>Documents</th>
<th>Purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product description and</td>
<td><strong>Marketing brochures</strong></td>
<td>Describe product specifications and benefits.</td>
</tr>
</tbody>
</table>
You can access the most up-to-date H3C product documentation on the World Wide Web at [http://www.h3c.com](http://www.h3c.com).

Click the links on the top navigation bar to obtain different categories of product documentation:

- **[Technical Support & Documents > Technical Documents]** – Provides hardware installation, software upgrading, and software feature configuration and maintenance documentation.
- **[Products & Solutions]** – Provides information about products and technologies, as well as solutions.
- **[Technical Support & Documents > Software Download]** – Provides the documentation released with the software version.

## Technical support

service@h3c.com

http://www.h3c.com
Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.
We appreciate your comments.
# Contents

## Configuring VLANs

- Introduction to VLAN ................................................. 1
- VLAN overview .......................................................... 1
- VLAN fundamentals .................................................... 2
- VLAN types ................................................................... 3
- Protocols and standards ............................................... 3

## Configuring basic VLAN settings

- Configure basic settings of a VLAN interface .................. 4
- VLAN interface overview ............................................... 4
- Configuration procedure ............................................... 4
- VLAN interface configuration example .......................... 5

## Configuring port-based VLANs

- Introduction to port-based VLAN .................................. 6
- Assigning an access port to a VLAN .............................. 8
- Assigning a trunk port to a VLAN ................................. 9
- Assigning a hybrid port to a VLAN ............................... 10
- Port-based VLAN configuration example ...................... 11

## MAC-based VLAN configuration

- Introduction to MAC-based VLAN ............................... 13
- Configuring a MAC-based VLAN ................................. 14
- MAC-based VLAN configuration example ..................... 15

## Displaying and maintaining VLANs

- Displaying and maintaining VLANs ............................. 18

## MAC address table configuration

- Overview ................................................................. 19
- types of MAC address table entries ............................... 20
- MAC address table-based frame forwarding .................. 20

## Configuring the MAC address table

- Configuring the MAC address table .............................. 20
- Disabling MAC address learning .................................. 21
- Configuring the aging timer for dynamic MAC address entries .......................................................... 22
- Configuring the MAC learning limit ............................. 23

## Displaying and maintaining MAC address tables

- Displaying and maintaining MAC address tables .......... 24

## Configuring the spanning tree

- Configuring the spanning tree .................................... 26
- STP .......................................................................... 26
- STP protocol packets .................................................. 26
- Basic concepts in STP .................................................. 27
- Calculation process of the STP algorithm ..................... 28
- RSTP ........................................................................ 33
- MSTP ........................................................................ 33
- STP and RSTP limitations ........................................... 33
- MSTP features .......................................................... 33
- MSTP basic concepts .................................................. 34
- How MSTP works ...................................................... 37
- Implementation of MSTP on routers ............................ 38

## Protocols and standards

- Protocols and standards ............................................... 38
- Spanning tree configuration task list ......................... 38
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring VLAN termination</td>
<td>119</td>
</tr>
<tr>
<td>Configuring QinQ</td>
<td>95</td>
</tr>
<tr>
<td>Configuring GVRP</td>
<td>107</td>
</tr>
<tr>
<td>Configuring BPDU tunneling</td>
<td>102</td>
</tr>
<tr>
<td>Configuring VLAN termination configuration examples</td>
<td>126</td>
</tr>
<tr>
<td>Ambiguous QinQ termination configuration example</td>
<td>128</td>
</tr>
<tr>
<td>Unambiguous QinQ termination configuration example</td>
<td>126</td>
</tr>
<tr>
<td>Configuring TPID for VLAN-tagged packets</td>
<td>121</td>
</tr>
<tr>
<td>Configuring unambiguous QinQ termination</td>
<td>125</td>
</tr>
<tr>
<td>Configuring ambiguous QinQ termination</td>
<td>126</td>
</tr>
<tr>
<td>VLAN termination configuration examples</td>
<td>126</td>
</tr>
</tbody>
</table>
Configuring VLANs

Introduction to VLAN

VLAN overview

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared in an Ethernet, network performance may degrade as the number of hosts on the network is increasing. If the number of the hosts in the network reaches a certain level, problems caused by collisions, broadcasts, and so on emerge, which may cause the network to malfunction. In addition to the function that suppresses collisions (which can also be achieved by interconnecting LANs), virtual LAN (VLAN) can isolate broadcast packets as well. VLAN divides a LAN into multiple logical LANs with each being a broadcast domain. Hosts in the same VLAN can communicate with each other like in a LAN. However, hosts from different VLANs cannot communicate directly. In this way, broadcast packets are confined to a single VLAN, as illustrated in the following figure.

Figure 1 A VLAN diagram

A VLAN can span across physical spaces. The hosts that reside in different network segments may belong to the same VLAN, users in a VLAN can be connected to the same switch, or span across multiple switches or routers.

VLAN technology has the following advantages:

- Broadcast traffic is confined to each VLAN, reducing bandwidth utilization and improving network performance.
- LAN security is improved. Packets in different VLANs are isolated at Layer 2. That is, users in a VLAN cannot communicate with users in other VLANs directly, unless Layer 3 network devices such as routers are used.
- A more flexible way to establish virtual workgroups. With VLAN technology, a virtual workgroup can be created spanning physical network segments. That is, users from the same workgroup do not have to be within the same physical area, making network construction and maintenance much easier and more flexible.
VLAN fundamentals

To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation.

The format of VLAN-tagged frames is defined in IEEE 802.1Q issued by the Institute of Electrical and Electronics Engineers (IEEE) in 1999.

In the header of a traditional Ethernet data frame, the field following the destination MAC address and the source MAC address is the Type field, which indicates the upper layer protocol type. Figure 2 illustrates the format of a traditional Ethernet frame, where DA stands for destination MAC address, SA stands for source MAC address, and Type refers to the upper layer protocol type of the frame.

Figure 2 The format of a traditional Ethernet frame

<table>
<thead>
<tr>
<th>DA&amp;SA</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
</table>

IEEE 802.1Q defines a four-byte VLAN Tag between the DA&SA field and the Type field to carry VLAN-related information, as shown in Figure 3.

Figure 3 The position and the format of VLAN tag

A VLAN tag comprises four fields: the tag protocol identifier (TPID) field, the Priority field, the canonical format indicator (CFI) field, and the VLAN ID field.

- The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN-tagged.
- The Priority field, three bits in length, indicates the 802.1p priority of a packet. For more information about packet priority, see ACL and QoS Configuration Guide.
- The CFI field, one bit in length, specifies whether or not the MAC addresses are encapsulated in standard format when packets are transmitted across different media. With the field set to 0, MAC addresses are encapsulated in standard format; with the field set to 1, MAC addresses are encapsulated in non-standard format. The filed is 0 by default.
- The VLAN ID field, 12 bits in length and with its value ranging from 0 to 4095, identifies the ID of the VLAN a packet belongs to. As VLAN IDs of 0 and 4095 are reserved by the protocol, the value of this field actually ranges from 1 to 4094.

A network device determines the VLAN to which a packet belongs by the VLAN ID field the packet carries. The VLAN tag determines the way a packet is processed. For more information, see “Introduction to port-based VLAN.”
NOTE:

- The Ethernet II encapsulation format is used here. Besides the Ethernet II encapsulation format, other encapsulation formats, including 802.2 LLC, 802.2 SNAP, and 802.3 raw, are also supported by Ethernet. The VLAN tag fields are also added to frames encapsulated in these formats for VLAN identification.
- For a frame with multiple VLAN tags, the network device handles it according to its outer-most VLAN tag, and transmits its inner VLAN tags as payload.
- VLAN 4094 is not available when different types of service cards are intermixed.

VLAN types

You can implement VLANs based on the following criteria:

- Port
- MAC address

Protocols and standards

- IEEE 802.1Q, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

Configuring basic VLAN settings

To configure basic VLAN settings:

<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-id1 [ to vlan-id2 ]</td>
<td>all }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, only the default VLAN (that is, VLAN 1) exists in the system. If the specified VLAN does not exist, this command creates the VLAN first.</td>
</tr>
<tr>
<td>3.</td>
<td>vlan vlan-id</td>
<td>Optional. By default, the VLAN ID is used as the name of a VLAN. For example, VLAN 0001.</td>
</tr>
<tr>
<td>4.</td>
<td>name text</td>
<td>Optional. By default, the VLAN ID is used as the description. For example, VLAN 0001.</td>
</tr>
<tr>
<td>5.</td>
<td>description text</td>
<td>Optional. By default, the VLAN ID is used as the description. For example, VLAN 0001.</td>
</tr>
</tbody>
</table>

NOTE:

The router does not support VLAN 4094 when it works in hybrid mode. For more information about system working modes, see Fundamentals Configuration Guide.
Configure basic settings of a VLAN interface

VLAN interface overview

For hosts of different VLANs to communicate, you must use a router or Layer 3 switch to perform layer 3 forwarding. To achieve this, VLAN interfaces are used.

VLAN interfaces are Layer 3 virtual interfaces used for Layer 3 interoperability between different VLANs. Each VLAN corresponds to one VLAN interface. After you assign an IP address to a VLAN interface, this interface can serve as the gateway for the network devices in the VLAN and allows IP address-based Layer 3 forwarding.

Configuration procedure

To perform basic VLAN interface configuration:

<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 VLAN interface view.</td>
<td>interface vlan-interface vlan-interface-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an IP address for the VLAN interface.</td>
<td>ip address ip-address { mask</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the description of the VLAN interface.</td>
<td>description text</td>
</tr>
<tr>
<td>5.</td>
<td>Set the MTU for the VLAN interface.</td>
<td>mtu size</td>
</tr>
<tr>
<td>6.</td>
<td>Restore the default settings for the VLAN interface.</td>
<td>default</td>
</tr>
<tr>
<td>7.</td>
<td>Bring up the VLAN interface.</td>
<td>undo shutdown</td>
</tr>
</tbody>
</table>

NOTE:

Before creating a VLAN interface, make sure that the corresponding VLAN already exists. Otherwise, the specified VLAN interface will not be created.
### VLAN interface configuration example

#### Network requirements
As shown in Figure 4, PC A is assigned to VLAN 5. PC B is assigned to VLAN 10. The PCs belong to different IP subnets and cannot communicate with each other.

Configure VLAN interfaces on Router A and configure the PCs to enable Layer 3 communication between the PCs.

*Figure 4 Network diagram*

#### Configuration procedure

1. **Configure Router A**
   
   # Create VLAN 5 and assign GigabitEthernet 3/1/1 to it.
   ```
   <RouterA> system-view
   [RouterA] vlan 5
   [RouterA-vlan5] port gigabitethernet 3/1/1
   # Create VLAN 10 and assign GigabitEthernet 3/1/2 to it.
   [RouterA-vlan5] vlan 10
   [RouterA-vlan10] port gigabitethernet 3/1/2
   [RouterA-vlan10] quit
   # Create VLAN-interface 5 and configure its IP address as 192.168.0.10/24.
   [RouterA] interface vlan-interface 5
   [RouterA-Vlan-interface5] ip address 192.168.0.10 24
   [RouterA-Vlan-interface5] quit
   # Create VLAN-interface 10 and configure its IP address as 192.168.1.20/24.
   [RouterA] interface vlan-interface 10
   [RouterA-Vlan-interface10] ip address 192.168.1.20 24
   [RouterA-Vlan-interface10] return
   ```

2. **Configure PC A**
   
   # Configure the default gateway of the PC as 192.168.0.10.

3. **Configure PC B**
   
   # Configure the default gateway of the PC as 192.168.1.20.

#### Verifying the configurations

1. The PCs can ping each other.
2. Display brief information about Layer 3 interfaces on Router A to verify the configuration.
<RouterA> display ip interface brief
*down: administratively down
(s): spoofing

<table>
<thead>
<tr>
<th>Interface</th>
<th>Physical</th>
<th>Protocol</th>
<th>IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan5</td>
<td>up</td>
<td>up</td>
<td>192.168.0.10</td>
<td>Vlan-inte...</td>
</tr>
<tr>
<td>Vlan10</td>
<td>up</td>
<td>up</td>
<td>192.168.1.20</td>
<td>Vlan-inte...</td>
</tr>
</tbody>
</table>

### Configuring port-based VLANs

#### Introduction to port-based VLAN

Port-based VLANs group VLAN members by port. A port forwards traffic for a VLAN only after it is assigned to the VLAN.

#### Port link type

You can configure the link type of a port as access, trunk, or hybrid. The three link types use different VLAN tag handling methods.

- An access port belongs to only one VLAN and sends traffic untagged. It is typically used to connect a terminal device unable to recognize VLAN tagged-packets or when there is no need to differentiate VLAN members. As shown in Figure 5, because Device A is connected with common PCs that cannot recognize VLAN tagged-packets, you need to configure Device A’s ports that connect the PCs as access ports.

- A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic of the port VLAN (PVID), traffic sent through a trunk port will be VLAN tagged. Usually, ports connecting network devices are configured as trunk ports. As shown in Figure 5, because Device A and Device B need to transmit packets of VLAN 2 and VLAN 3, you need to configure the ports connecting Device A and Device B as trunk ports, and assign them to VLAN 2 and VLAN 3.

- Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. Unlike a trunk port, a hybrid port allows traffic of all VLANs to pass through untagged. Usually, hybrid ports are configured to connect network devices whose support for VLAN tagged-packets you are uncertain about. As shown in Figure 5, Device B connects a small-sized LAN in which some PCs belong to VLAN 2 while some other PCs belong to VLAN 3. In this case, you need to configure Device B’s port connecting the LAN as a hybrid port that allows packets of VLAN 2 and VLAN 3 to pass through untagged.
You can configure a port VLAN (PVID) for a port. By default, VLAN 1 is the PVID for all ports.

- An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port. The PVID of the access port changes along with the VLAN to which the port belongs.
- A trunk or hybrid port can join multiple VLANs, and you can configure a PVID for the port.
- You can use a nonexistent VLAN as the PVID for a hybrid or trunk port but not for an access port. Therefore, after you remove the VLAN that an access port resides in with the `undo vlan` command, the PVID of the port changes to VLAN 1. The removal of a VLAN specified as the PVID of a trunk or hybrid port, however, does not affect the setting of the PVID on the port.

**NOTE:**

- It is recommended that you set the same PVID for the local and remote ports.
- Make sure that a port is assigned to its PVID. Otherwise, when receiving frames tagged with the PVID or untagged frames (including protocol packets such as MSTP BPDUs), the port filters out these frames.

Ports of different link types handle frames as follows:

<table>
<thead>
<tr>
<th>Port type</th>
<th>Actions (in the inbound direction)</th>
<th>Actions (in the outbound direction)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Untagged frame</td>
<td>Tagged frame</td>
</tr>
<tr>
<td>Access</td>
<td>Tag the frame with the PVID tag.</td>
<td></td>
</tr>
</tbody>
</table>
  - Receive the frame if its VLAN ID is the same as the PVID.  
  - Drop the frame if its VLAN ID is different from the PVID. | Remove the VLAN tag and send the frame. |
<table>
<thead>
<tr>
<th>Port type</th>
<th>Actions (in the inbound direction)</th>
<th>Actions (in the outbound direction)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Untagged frame</td>
<td>Tagged frame</td>
</tr>
<tr>
<td>Trunk</td>
<td>Check whether the PVID is permitted on the port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If yes, tag the frame with the PVID tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If not, drop the frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Receive the frame if its VLAN is carried on the port.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drop the frame if its VLAN is not carried on the port.</td>
<td></td>
</tr>
<tr>
<td>Hybrid</td>
<td>Send the frame if its VLAN is carried on the port.</td>
<td>The frame is sent with the VLAN tag removed or intact depending on your configuration with the <code>port hybrid vlan</code> command. This is true of the PVID.</td>
</tr>
</tbody>
</table>

Assigning an access port to a VLAN

You can assign an access port to a VLAN in VLAN view, interface view (including Ethernet interface view, Layer 2 aggregate interface view, and Layer 2 VE interface view), or port group view.

To 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><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>vlan vlan-id</code></td>
<td>If the specified VLAN does not exist, this command creates the VLAN first.</td>
</tr>
<tr>
<td>3.</td>
<td><code>port interface-list</code></td>
<td>By default, all ports belong to VLAN 1.</td>
</tr>
</tbody>
</table>

To assign an access port (in interface view) or a group of ports (in port group view) to a VLAN:

<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>
### Step 2. Enter interface view or port group view.

- Enter Ethernet interface view:
  ```
  interface interface-type
  interface-number
  ```
- Enter Layer 2 aggregate interface view:
  ```
  interface bridge-aggregation
  interface-number
  ```
- Enter Layer 2 virtual Ethernet interface view:
  ```
  interface ve-bridge
  interface-number
  ```
- Enter port group view:
  ```
  port-group manual
  port-group-name
  ```

Use any one of the commands.

### Step 3. Configure the link type of the port or ports as access.

- **Command:** `port link-type access`

Optional. The link type of a port is access by default.

### Step 4. Assign the current access port(s) to a VLAN.

- **Command:** `port access vlan vlan-id`

Optional. By default, all access ports belong to VLAN 1.

### NOTE:

- Before assigning an access port to a VLAN, create the VLAN first.
- In VLAN view, you can assign only Layer 2 Ethernet interfaces to the current VLAN.

## Assigning a trunk port to a VLAN

A trunk port can carry multiple VLANs. You can assign it to a VLAN in interface view (including Ethernet interface view, Layer 2 aggregate interface view, and Layer 2 VE interface view) or port group view.

To assign a trunk port to one or multiple VLANs:

### Step 1. Enter system view.

- **Command:** `system-view`

<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 interface view or port group view.

- Enter Ethernet interface view:
  
  ```
  interface interface-type
  interface-number
  ```

- Enter Layer 2 aggregate interface view:
  
  ```
  interface bridge-aggregation
  interface-number
  ```

- Enter Layer 2 virtual Ethernet interface view:
  
  ```
  interface ve-bridge
  interface-number
  ```

- Enter port group view:
  
  ```
  port-group manual
  port-group-name
  ```

3. Configure the link type of the port or ports as trunk.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>port link-type trunk</td>
<td>N/A</td>
</tr>
</tbody>
</table>

4. Assign the trunk port(s) to the specified VLAN(s).

   ```
   port trunk permit vlan { vlan-id-list | all }
   ```

   By default, a trunk port carries only VLAN 1.

5. Configure the PVID of the trunk port(s).

   ```
   port trunk pvid vlan vlan-id
   ```

   Optional. By default, the PVID is VLAN 1.

**NOTE:**

- To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.
- After configuring the PVID for a trunk port, you must use the `port trunk permit vlan` command to configure the trunk port to allow packets from the PVID to pass through, so that the egress port can forward packets from the PVID.

**Assigning a hybrid port to a VLAN**

A hybrid port can carry multiple VLANs. You can assign it to a VLAN in interface view (including Ethernet interface view, Layer 2 aggregate interface view, and Layer 2 VE interface view) or port group view.

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>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter interface view or port group view.</td>
<td>Use any one of the commands.</td>
</tr>
<tr>
<td></td>
<td>• Enter Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface interface-type</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface bridge-aggregation</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 virtual Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface ve-bridge</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>port-group manual</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>port-group-name</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the link type of the port(s) as hybrid.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><code>port link-type hybrid</code></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Assign the hybrid port(s) to the specified VLAN(s).</td>
<td>By default, a hybrid port only permits the packets of VLAN 1 to pass through untagged.</td>
</tr>
<tr>
<td></td>
<td>`port hybrid vlan vlan-id-list { tagged</td>
<td>untagged }`</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the PVID of the hybrid port.</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td><code>port hybrid pvid vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the PVID is VLAN 1.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

- To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.
- Before assigning a hybrid port to a VLAN, create the VLAN first.
- After configuring the PVID for a hybrid port, you must use the `port hybrid vlan` command to configure the hybrid port to allow packets from the PVID to pass through, so that the egress port can forward packets from the PVID.

---

### Port-based VLAN configuration example

**Network requirements**

As shown in Figure 6, Host A and Host C belong to Department A, and access the enterprise network through different routers. Host B and Host D belong to Department B. They also access the enterprise network through different routers.

To ensure communication security and avoid broadcast storms, VLANs are configured in the enterprise network to isolate Layer 2 traffic of different departments. VLAN 100 is assigned to Department A, and VLAN 200 is assigned to Department B.

Make sure that hosts within the same VLAN can communicate with each other, that is, Host A can communicate with Host C, and Host B can communicate with Host D.
Configuration procedure

1. Configure Device A:

   # Create VLAN 100, and assign port GigabitEthernet 3/1/1 to VLAN 100.
   
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] port gigabitEthernet 3/1/1
   [DeviceA-vlan100] quit

   # Create VLAN 200, and assign port GigabitEthernet 3/1/2 to VLAN 200.
   
   [DeviceA] vlan 200
   [DeviceA-vlan200] port gigabitEthernet 3/1/2
   [DeviceA-vlan200] quit

   # Configure port GigabitEthernet 3/1/3 as a trunk port, and assign it to VLANs 100 and 200, thus enabling GigabitEthernet 3/1/3 to forward traffic of VLANs 100 and 200 to Device B.
   
   [DeviceA] interface gigabitEthernet 3/1/3
   [DeviceA-GigabitEthernet3/1/3] port link-type trunk
   [DeviceA-GigabitEthernet3/1/3] port trunk permit vlan 100 200
   Please wait... Done.

2. Configure Device B:

   Configure Device B as you configure Device A.

3. Configure hosts:

   Configure Host A and Host C to be on the same network segment, 192.168.100.0/24 for example. Configure Host B and Host D to be on the same network segment, 192.168.200.0/24 for example.

Verifying the configurations

1. Host A and Host C can ping each other successfully, but they both fail to ping Host B. Host B and Host D can ping each other successfully, but they both fail to ping Host A.

2. Check whether the configuration is successful by displaying relevant VLAN information.

   # Display information about VLANs 100 and 200 on Device A:
   
   [DeviceA-GigabitEthernet3/1/3] display vlan 100
   VLAN ID: 100
   VLAN Type: static
   Route Interface: not configured
   Description: VLAN 0100
   Name: VLAN 0100
   Broadcast MAX-ratio: 100%
MAC-based VLAN configuration

Introduction to MAC-based VLAN

The MAC-based VLAN feature assigns hosts to a VLAN based on their MAC addresses. This feature is mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Static MAC-based VLAN assignment

Static MAC-based VLAN assignment applies to networks containing a small number of VLAN users. In such a network, you can create a MAC address-to-VLAN map containing multiple MAC address-to-VLAN entries on a port, enable MAC-based VLAN on the port, and assign the port to MAC-based VLans.

With static MAC-based VLAN assignment configured on a port, the device processes received frames by using the following guidelines:

- When the port receives an untagged frame, the device looks up the MAC address-to-VLAN map based on the source MAC address of the frame for a match. The device first performs a fuzzy match. In the fuzzy match, the device searches the MAC address-to-VLAN entries whose masks are not all-Fs and performs a logical AND operation on the source MAC address and each mask. If the result of an AND operation matches the corresponding MAC address, the device tags the frame with the corresponding VLAN ID. If the fuzzy match fails, the device performs an exact match. In the exact match, the device searches the MAC address-to-VLAN entries whose masks are all-Fs. If the MAC address of a MAC address-to-VLAN entry matches the source MAC address of the untagged frame, the device tags the frame with the corresponding VLAN ID. If no match is found, the device assigns a VLAN to the frame by using other criteria, such as IP address. If no match is found, the device tags the frame with the PVID of the receiving port and forwards the frame.

- When the port receives a tagged frame, the port forwards the frame if the VLAN ID of the frame is permitted by the port, or otherwise drops the frame.

Dynamic MAC-based VLAN

You can use dynamic MAC-based VLAN with access authentication (such as 802.1X authentication based on MAC addresses) to implement secure, flexible terminal access. After configuring dynamic
MAC-based VLAN on the router, you must configure the MAC address-to-VLAN entries on the access authentication server.

When a user passes authentication of the access authentication server, the router obtains VLAN information from the server, generates a MAC address-to-VLAN entry by using the source MAC address of the user packet and the VLAN information, and assigns the port to the MAC-based VLAN. When the user goes offline, the router automatically deletes the MAC address-to-VLAN entry, and removes the port from the MAC-based VLAN.

NOTE:
For more information about access authentication, see Security Configuration Guide.

Configuring a MAC-based VLAN

NOTE:
- The router supports MAC-based VLAN only when its system working mode is SPC.
- MAC-based VLANs are available only on hybrid ports.
- Because MAC-based dynamic port assignment is mainly configured on the downlink ports of user access devices, do not enable this function together with link aggregation.

To configure 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>2.</td>
<td>Associate MAC addresses with a VLAN.</td>
<td>mac-vlan mac-address mac-address vlan vlan-id [ priority priority ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Ethernet interface view or port group view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td>port-group manual port-group-name</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the link type of the port(s) as hybrid.</td>
<td>port link-type hybrid</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the current hybrid port(s) to permit packets of specific MAC-based VLANs to pass through.</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>
</tbody>
</table>

To configure dynamic 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>
<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 Ethernet interface view or port group view.</td>
<td>Use either command.</td>
</tr>
<tr>
<td></td>
<td>• Enter Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface interface-type</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>port-group manual</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>port-group-name</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the link type of the port(s) as hybrid.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><code>port link-type hybrid</code></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Configure the hybrid port(s) to permit packets from specific MAC-based VLANs to pass through.</td>
<td>By default, a hybrid port only permits the packets of VLAN 1 to pass through.</td>
</tr>
<tr>
<td></td>
<td><code>port hybrid vlan vlan-id-list</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`{ tagged</td>
<td>untagged }`</td>
</tr>
<tr>
<td>5.</td>
<td>Enable the MAC-based VLAN feature.</td>
<td>By default, the MAC-based VLAN feature is disabled.</td>
</tr>
<tr>
<td></td>
<td><code>mac-vlan enable</code></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Configure 802.1X/MAC/portal authentication or any combination.</td>
<td>For more information, see Security Command Reference.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Security Command Reference.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**MAC-based VLAN configuration example**

**NOTE:**
- The router supports MAC-based VLAN only when its system working mode is SPC.
- MAC-based VLANs are available only on hybrid ports.

**Network requirements**

As shown in Figure 7,
- GigabitEthernet 3/1/1 of Device A and Device C are each connected to a meeting room. Laptop 1 (000d-88f8-4e71) and Laptop 2 (0014-222c-aa69) are used for meeting and may be used in any of the two meeting rooms.
- Laptop 1 and Laptop 2 are owned by different departments. The two departments use VLAN 100 and VLAN 200 respectively.

Configure MAC-based VLAN so that each laptop can access only its own department server no matter which meeting room it is used in.
Figure 7 Network diagram

Configuration consideration

- Create VLANs 100 and 200.
- Configure the uplink ports of Device A and Device C as trunk ports, and assign them to VLANs 100 and 200.
- Configure the downlink ports of Device B as trunk ports, and assign them to VLANs 100 and 200. Assign the uplink ports of Device B to VLANs 100 and 200.
- Associate the MAC address of Laptop 1 with VLAN 100, and the MAC address of Laptop 2 with VLAN 200.

Configuration procedure

1. Configure Device A:

```bash
# Create VLANs 100 and 200.
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 200
[DeviceA-vlan200] quit

# Associate the MAC address of Laptop 1 with VLAN 100, and the MAC address of Laptop 2 with VLAN 200.
[DeviceA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[DeviceA] mac-vlan mac-address 0014-222c-aa69 vlan 200

# Configure Laptop 1 and Laptop 2 to access the network through GigabitEthernet 3/1/1: Configure GigabitEthernet 3/1/1 as a hybrid port that sends packets of VLANs 100 and 200 untagged, and enable MAC-based VLAN on it.
[DeviceA] interface GigabitEthernet 3/1/1
[DeviceA-GigabitEthernet3/1/1] port link-type hybrid
[DeviceA-GigabitEthernet3/1/1] port hybrid vlan 100 200 untagged
```
Please wait... Done.

[DeviceA-GigabitEthernet3/1/1] mac-vlan enable
[DeviceA-GigabitEthernet3/1/1] quit

# Configure the uplink port GigabitEthernet 3/1/2 as a trunk port, and assign it to VLANs 100 and 200, so that the laptops can access Server 1 and Server 2.

[DeviceA] interface GigabitEthernet 3/1/2
[DeviceA-GigabitEthernet3/1/2] port link-type trunk
[DeviceA-GigabitEthernet3/1/2] port trunk permit vlan 100 200
[DeviceA-GigabitEthernet3/1/2] quit

2. Configure Device B:

# Create VLANs 100 and 200. Assign GigabitEthernet 3/1/13 to VLAN 100, and GigabitEthernet 3/1/14 to VLAN 200.

<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port GigabitEthernet 3/1/13
[DeviceB-vlan100] quit
[DeviceB] vlan 200
[DeviceB-vlan200] port GigabitEthernet 3/1/14
[DeviceB-vlan200] quit

# Configure GigabitEthernet 3/1/3 and GigabitEthernet 3/1/4 as trunk ports, and assign them to VLANs 100 and 200.

[DeviceB] interface GigabitEthernet 3/1/3
[DeviceB-GigabitEthernet3/1/3] port link-type trunk
[DeviceB-GigabitEthernet3/1/3] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet3/1/3] quit
[DeviceB] interface GigabitEthernet 3/1/4
[DeviceB-GigabitEthernet3/1/4] port link-type trunk
[DeviceB-GigabitEthernet3/1/4] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet3/1/4] quit

3. Configure Device C:

Configure Device C as you configure Device A.

Verifying the configurations

1. Laptop 1 can access Server 1 only, and Laptop 2 can access Server 2 only.

2. On Device A and Device C, you can see that VLAN 100 is associated with the MAC address of Laptop 1, and VLAN 200 is associated with the MAC address of Laptop 2.

[DeviceA] display mac-vlan all
The following MAC VLAN addresses exist:
S:Static D:Dynamic

<table>
<thead>
<tr>
<th>MAC ADDR</th>
<th>MASK</th>
<th>VLAN ID</th>
<th>PRIO</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>000d-88f8-4e71</td>
<td>ffff-ffff-ffff</td>
<td>100</td>
<td>0</td>
<td>S</td>
</tr>
<tr>
<td>0014-222c-aa69</td>
<td>ffff-ffff-ffff</td>
<td>200</td>
<td>0</td>
<td>S</td>
</tr>
</tbody>
</table>

Total MAC VLAN address count:2
Configuration guidelines

1. MAC-based VLAN can be configured only on hybrid ports.
2. MAC-based VLAN is typically configured on the downlink ports of access layer devices, and hence cannot be configured together with the link aggregation function.

Displaying and maintaining VLANs

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display VLAN information.</td>
<td>display vlan [ vlan-id1 [ to vlan-id2 ]</td>
<td>all</td>
</tr>
<tr>
<td>Display VLAN interface information.</td>
<td>display interface [ vlan-interface ]</td>
<td>[ brief</td>
</tr>
<tr>
<td>Display hybrid ports or trunk ports on the router.</td>
<td>display port { hybrid</td>
<td>trunk }</td>
</tr>
<tr>
<td>Display MAC address-to-VLAN entries.</td>
<td>display mac-vlan all</td>
<td>dynamic</td>
</tr>
<tr>
<td>Display all interfaces with MAC-based VLAN enabled.</td>
<td>display mac-vlan interface [</td>
<td></td>
</tr>
<tr>
<td>Clear statistics on a port.</td>
<td>reset counters interface vlan-interface [ vlan-interface-id ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

NOTE:
The *reset counters interface* command clears statistics on VLAN interfaces. For more information, see *Interface Command Reference.*
MAC address table configuration

NOTE:

- MAC address table configuration applies only to Layer 2 Ethernet ports, Layer 2 virtual Ethernet (VE) interfaces, and Layer 2 aggregate interfaces.
- This document covers only the configuration of unicast MAC address table entries, including static, dynamic, and blackhole MAC address table entries.

Overview

A MAC address table is maintained for frame forwarding. Each entry in this table indicates the following information:

- The MAC address of a connected network device
- The interface to which the device is connected
- The VLAN to which the interface belongs

When forwarding a frame, the router first looks up the MAC address table by the destination MAC address of the frame for the outgoing port. If the outgoing port is found, the frame is forwarded rather than broadcast, so broadcasts are reduced.

How a MAC address table entry is created

A MAC address table entry can be dynamically learned or manually configured.

Dynamically learning MAC address entries

Usually, a router can populate its MAC address table automatically by learning the source MAC addresses of incoming frames on each port.

When a frame arrives at a port, Port A for example, the router performs the following tasks:

1. Checks the source MAC address (MAC-SOURCE for example) of the frame.
2. Looks up the source MAC address in the MAC address table.
   - If an entry is found, the router updates the entry.
   - If no entry is found, the router adds an entry for MAC-SOURCE and Port A.
3. After learning this source MAC address, when the router receives a frame destined for MAC-SOURCE, it finds the MAC-SOURCE entry in the MAC address table and forwards the frame out Port A.

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

To adapt to network changes, MAC address table entries must be constantly updated. Each dynamically learned MAC address table entry has an aging timer. If an entry is not updated when the aging timer expires, it is deleted. If it updates before the aging timer expires, the aging timer restarts.
Manually configuring MAC address entries

With dynamic MAC address learning, a router does not distinguish illegitimate frames from legitimate frames. This causes security hazards. For example, if a hacker sends frames with a forged source MAC address to a port different from the one where the real MAC address is connected, the router will create an entry for the forged MAC address, and will forward frames destined for the legal user to the hacker instead.

To enhance the security of a port, you can manually add MAC address entries in the MAC address table of the router to bind specific user devices to the port. Because manually configured entries have higher priority than the dynamically learned ones, this prevents hackers from stealing data using forged MAC addresses.

Types of MAC address table entries

A MAC address table may contain these types of entries:

- **Static entries**—Static entries are manually configured and never age out.
- **Dynamic entries**—Dynamic entries can be manually configured or dynamically learned and may age out.
- **Blackhole entries**—Blackhole entries are manually configured and never age out. Blackhole entries are configured for filtering out frames with specific source or destination MAC addresses. For example, to block all packets destined for a specific user for security concerns, you can configure the MAC address of this user as a destination blackhole MAC address entry.

**NOTE:**

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

MAC address table-based frame forwarding

When forwarding a frame, the router adopts the following two forwarding modes based on the MAC address table:

- **Unicast mode**—If an entry is available for the destination MAC address, the router forwards the frame out the outgoing interface indicated by the MAC address table entry.
- **Broadcast mode**—If the router receives a frame with an all-ones destination address, or no entry is available for the destination MAC address, the router broadcasts the frame to all the interfaces except the receiving interface.

Configuring the MAC address table

The configuration tasks discussed in the following sections are all optional and can be performed in any order.

Configuring MAC address table entries

To fence off MAC address spoofing attacks and improve port security, you can manually add MAC address table entries to bind ports with MAC addresses.

You can also configure blackhole MAC address entries to filter out packets with certain source or destination MAC addresses.
Add or modify a static, dynamic, or blackhole MAC address table entry globally

To add or modify a static, dynamic, or blackhole MAC address table entry in system 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>Add or modify a dynamic or static MAC address entry.</td>
<td>mac-address {dynamic</td>
</tr>
<tr>
<td>3.</td>
<td>Add or modify a blackhole MAC address entry.</td>
<td>mac-address blackhole mac-address vlan vlan-id</td>
</tr>
</tbody>
</table>

Add or modify a static or dynamic MAC address table entry on an interface

To add or modify a static or dynamic MAC address table entry 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 interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Add or modify a MAC address entry.</td>
<td>mac-address {dynamic</td>
</tr>
</tbody>
</table>

Disabling MAC address learning

You may need to disable MAC address learning sometimes to prevent the MAC address table from being saturated, for example, when your router is being attacked by a large amount of packets with different source MAC addresses.

Disabling MAC address learning on ports

After enabling global MAC address learning, you may disable the function on a single port, or on all ports in a port group as needed.

To disable MAC address learning on a Layer 2 Ethernet port, port group, Layer 2 VE interface, or 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>system-view</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
2. | Enter interface view or port group view. | Use any command. The configuration you make in Layer 2 Ethernet interface view, Layer 2 VE interface view, or Layer 2 aggregate interface view takes effect on the current interface only. Configuration made in port group view takes effect on all the member ports in the port group.

3. | Disable MAC address learning. | By default, MAC address learning is enabled on ports.

**NOTE:**
For more information about port group configuration, see *Interface Configuration Guide*.

**Disabling MAC address learning on a VLAN**

You may disable MAC address learning on a per-VLAN basis. To disable MAC address learning on a VLAN:

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
2. | Enter VLAN view. | vlan vlan-id | N/A
3. | Disable MAC address learning on the VLAN. | mac-address mac-learning disable | By default, MAC address learning is enabled.

**Configuring the aging timer for dynamic MAC address entries**

The MAC address table uses an aging timer for dynamic MAC address entries for security and efficient use of table space. If a dynamic MAC address entry has failed to update before the aging timer expires, the router deletes the entry. This aging mechanism ensures that the MAC address table could promptly update to accommodate latest network changes.

Set the aging timer appropriately. Too long an aging interval may cause the MAC address table to retain outdated entries, exhaust the MAC address table resources, and fail to update its entries to accommodate the latest network changes. Too short an interval may result in removal of valid entries, causing unnecessary broadcasts, which may affect router performance.

To configure the aging timer for dynamic MAC address entries:

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
2. | Configure the aging timer for dynamic MAC address entries. | mac-address timer { aging seconds | no-aging } | Optional. The default setting is 300 seconds.
NOTE:

- The MAC address aging timer takes effect globally only on dynamic MAC address entries (learned or administratively configured).
- You can reduce broadcasts on a stable network by disabling the aging timer to prevent dynamic entries from unnecessarily aging out. By reducing broadcasts, you improve not only network performance, but also security, because the chances for a data packet to reach unintended destinations are reduced.

Configuring the MAC learning limit

Configuring the MAC learning limit on ports

As the MAC address table grows, the forwarding performance of your router may degrade. To prevent the MAC address table from getting so large that the forwarding performance is affected, you can limit the number of MAC addresses that can be learned on a port.

To configure the MAC learning limit on a Layer 2 Ethernet interface, Layer 2 VE interface, Layer 2 aggregate interface, or all ports in a port 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 interface view or port group view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 Ethernet interface view, Layer 2 VE interface view, or Layer 2 aggregate interface view:</td>
<td>Interface command</td>
</tr>
<tr>
<td></td>
<td>interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td>Port group command</td>
</tr>
<tr>
<td></td>
<td>port-group manual port-group-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the MAC learning limit on the interface or port group, and specify whether or not frames with unknown source MAC addresses can be forwarded when the MAC learning limit is reached.</td>
<td>mac-address max-mac-count { count</td>
</tr>
</tbody>
</table>

Configuring the MAC learning limit on a VLAN

You may also limit the number of MAC addresses that can be learned on a per-VLAN basis.

To configure the MAC learning limit 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>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
</tbody>
</table>
3. Configure the MAC learning limit on the VLAN, and specify whether or not frames with unknown source MAC addresses can be forwarded in the VLAN when the MAC learning limit is reached.

```
mac-address
max-mac-count { count | disable-forwarding }
```

By default, the maximum number of source MAC addresses that can be learned on a VLAN is not specified.

## Displaying and maintaining MAC address tables

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

## MAC address table configuration example

### Network requirements

As shown in Figure 8,

- The MAC address of a host (Host A) is 000f-e235-dc71 and belongs to VLAN 1. It is connected to GigabitEthernet 3/1/10 of the router. To prevent MAC address spoofing, add a static entry for the host in the MAC address table of the router.
- The MAC address of another host (Host B) is 000f-e235-abcd and belongs to VLAN 1. For security, because this host once behaved suspiciously on the network, add a destination blackhole MAC address entry for the host MAC address, so all packets destined for the host will be dropped.
- Set the aging timer for dynamic MAC address entries to 500 seconds.
Figure 8 Network diagram

Configuration procedure

# Add a static MAC address entry.
<Sysname> system-view
[Sysname] mac-address static 000f-e235-dc71 interface GigabitEthernet 3/1/10 vlan 1

# Add a destination blackhole MAC address entry.
[Sysname] mac-address blackhole 000f-e235-abcd vlan 1

# Set the aging timer for dynamic MAC address entries to 500 seconds.
[Sysname] mac-address timer aging 500

# Display the MAC address entry for port GigabitEthernet 3/1/10.
[Sysname] display mac-address interface GigabitEthernet 3/1/10
MAC ADDR          VLAN ID  STATE            PORT INDEX             AGING TIME(s)
000f-e235-dc71    1        Config static    GigabitEthernet3/1/10  NOAGED
---  1 mac address(es) found on port GigabitEthernet3/1/10 ---

# Display information about the destination blackhole MAC address table.
[Sysname] display mac-address blackhole
MAC ADDR        VLAN ID    STATE            PORT INDEX             AGING TIME
000f-e235-abcd  1          Blackhole        N/A                    NOAGED
---  1 mac address(es) found  ---

# View the aging time of dynamic MAC address entries.
[Sysname] display mac-address aging-time
Mac address aging time: 500s
Configuring the spanning tree

As a Layer 2 management protocol, the Spanning Tree Protocol (STP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the mean time, allows for link redundancy.

STP evolves as the network grows. The later versions of STP are the Rapid Spanning Tree Protocol (RSTP) 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 local area network (LAN). Routers running this protocol detect loops in the network by exchanging information with one another and 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 and prevents decreased performance of network devices caused by duplicate packets received.

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

STP protocol packets

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

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

In STP, BPDUs have the following types:

- **Configuration BPDUs**—Used for calculating a spanning tree and maintaining the spanning tree topology.
- **Topology change notification (TCN) BPDUs**—Used for notifying the involved routers of network topology changes, if any.

A configuration BPDU contains the following information for network devices to complete spanning tree calculation:

- **Root bridge ID**—Comprises the priority and MAC address of the root bridge.
- **Root path cost**—Cost of the path to the root bridge.
- **Designated bridge ID**—Comprises the priority and MAC address of the designated bridge.
- **Designated port ID**—Comprises the port priority and global port number.
- **Message age**—Times that the configuration BPDU has been forwarded on the network.
- **Max age**—Maximum age of the configuration BPDU.
- **Hello time**—Transmission interval of the configuration BPDU.
- **Forward delay**—Delay before a port transitions to the forwarding state.
Basic concepts in STP

Root bridge

A tree network must have a root bridge.

There is only one root bridge in the entire network. The root bridge is not fixed, but can change along with changes of the network topology.

Upon initialization of a network, each router generates and sends out configuration BPDUs periodically with itself as the root bridge. After network convergence, only the root bridge generates and sends out configuration BPDUs at a certain interval, and the other routers 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 1 Description of designated bridges and designated ports

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

As shown in Figure 9, Device B and Device C are directly connected to a LAN. If Device A forwards BPDUs to Device B through port A1, the designated bridge for Device B is Device A, and the designated port of Device B is port A1 on Device A. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port for the LAN is port B2 on Device B.

Figure 9 A schematic diagram of designated bridges and designated ports

Path cost

Path cost is a reference value used for link selection in STP. By calculating path costs, STP selects relatively robust links and blocks redundant links, and finally prunes the network into a loop-free tree.
Calculation process of the STP algorithm

The STP algorithm uses the following calculation process:

1. **Initial state**
   
   Upon initialization of a router, each port generates a BPDU with the router as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the port itself.

2. **Selection of the root bridge**
   
   Initially, each STP-enabled router on the network assumes itself to be the root bridge, with the root bridge ID being its own device ID. By exchanging configuration BPDUs, the routers compare their root bridge IDs to elect the router with the smallest root bridge ID as the root bridge.

3. **Selection of the root port and designated ports on a non-root router**
   
   Table 2 describes the process of selecting the root port and designated ports.

<table>
<thead>
<tr>
<th>Table 2 Selection of the root port and designated ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

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

<table>
<thead>
<tr>
<th>Table 3 Selection of the optimum configuration BPDU</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The router compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

NOTE:
The following are the principles of configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.
- If all configuration BPDUs have the same root bridge ID, their root path costs are compared. For example, the root path cost in a configuration BPDU plus the path cost of a receiving port is $S$. The configuration BPDU with the smallest $S$ value has the highest priority.
- If all configuration BPDUs have the same ports value, their designated bridge IDs, designated port IDs, and the IDs of the receiving ports are compared in sequence. The configuration BPDU containing a smaller ID wins out.

A tree-shape topology forms when the root bridge, root ports, and designated ports are selected. The following describes with an example how the STP algorithm works.

Figure 10 The STP algorithm

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

Table 4 Initial state of each device

<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>
NOTE:
In Table 4, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

5. Comparison process and result on each device

Table 5 Comparison process and result on each device

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
</table>
| Device A| • Port A1 receives the configuration BPDU of Port B1 \(\{1, 0, 1, \text{Port B1}\}\), finds that its existing configuration BPDU \(\{0, 0, 0, \text{Port A1}\}\) is superior to the received configuration BPDU, and discards the received one.  
• Port A2 receives the configuration BPDU of Port C1 \(\{2, 0, 2, \text{Port C1}\}\), finds that its existing configuration BPDU \(\{0, 0, 0, \text{Port A2}\}\) is superior to the received configuration BPDU, and discards the received one.  
• Device A finds that it is both the root bridge and designated bridge in the configuration BPDU of all its ports, and considers itself as the root bridge. It does not change the configuration BPDU of any port and starts to periodically send out configuration BPDU. | • Port A1: \(\{0, 0, 0, \text{Port A1}\}\)  
• Port A2: \(\{0, 0, 0, \text{Port A2}\}\) |
| Device B| • Port B1 receives the configuration BPDU of Port A1 \(\{0, 0, 0, \text{Port A1}\}\), finds that the received configuration BPDU is superior to its existing configuration BPDU \(\{1, 0, 1, \text{Port B1}\}\), and updates its configuration BPDU.  
• Port B2 receives the configuration BPDU of Port C2 \(\{2, 0, 2, \text{Port C2}\}\), finds that its existing configuration BPDU \(\{1, 0, 1, \text{Port B2}\}\) is superior to the received configuration BPDU, and discards the received one.  
• Device B compares the configuration BPDU of all its ports, decides that the configuration BPDU of Port B1 is the optimum, and 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 \(\{0, 5, 1, \text{Port B2}\}\), and compares it with the existing configuration BPDU of Port B2 \(\{1, 0, 1, \text{Port B2}\}\). Device B finds that the calculated one is superior, decides that Port B2 is the designated port, replaces the configuration BPDU on Port B2 with the calculated one, and periodically sends out the calculated configuration BPDU. | • Port B1: \(\{0, 0, 0, \text{Port A1}\}\)  
• Port B2: \(\{1, 0, 1, \text{Port B2}\}\)  
• Root port (Port B1): \(\{0, 0, 0, \text{Port A1}\}\)  
• Designated port (Port B2): \(\{0, 5, 1, \text{Port B2}\}\) |
<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>Configuration BPDU on ports after comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port C1 receives the configuration BPDU of Port A2 (0, 0, 0, Port A2), finds that the received configuration BPDU is superior to its existing configuration BPDU (2, 0, 2, Port C1), and updates its configuration BPDU.</td>
<td>Port C1: {0, 0, 0, Port A2}</td>
<td></td>
</tr>
<tr>
<td>Port C2 receives the original configuration BPDU of Port B2 (1, 0, 1, Port B2), finds that the received configuration BPDU is superior to the existing configuration BPDU (2, 0, 2, Port C2), and updates its configuration BPDU.</td>
<td>Port C2: {1, 0, 1, Port B2}</td>
<td></td>
</tr>
<tr>
<td>Device C compares the configuration BPDU of all its ports, decides that the configuration BPDU of Port C1 is the optimum, and selects Port C1 as the root port with the configuration BPDU unchanged.</td>
<td>Root port (Port C1): {0, 0, 0, Port A2}</td>
<td></td>
</tr>
<tr>
<td>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), and compares it with the existing configuration BPDU of Port C2 (1, 0, 1, Port B2). Device C finds 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.</td>
<td>Designated port (Port C2): {0, 10, 2, Port C2}</td>
<td></td>
</tr>
<tr>
<td>Port C2 receives the updated configuration BPDU of Port B2 (0, 5, 1, Port B2), finds that the received configuration BPDU is superior to its existing configuration BPDU (0, 10, 2, Port C2), and updates its configuration BPDU.</td>
<td>Port C1: {0, 0, 0, Port A2}</td>
<td></td>
</tr>
<tr>
<td>Port C1 receives a periodic configuration BPDU (0, 0, 0, Port A2) from Port A2, finds that it is the same as the existing configuration BPDU, and discards the received one.</td>
<td>Port C2: {0, 5, 1, Port B2}</td>
<td></td>
</tr>
<tr>
<td>Device C finds that the root path cost of Port C1 (10) (root path cost of the received configuration BPDU (0) plus path cost of Port C1 (10)) is larger than that of Port C2 (9) (root path cost of the received configuration BPDU (5) plus path cost of Port C2 (4)), decides that the configuration BPDU of Port C2 is the optimum, and selects Port C2 as the root port with the configuration BPDU unchanged.</td>
<td>Blocked port (Port C1): {0, 0, 0, Port A2}</td>
<td></td>
</tr>
<tr>
<td>Based on the configuration BPDU and path cost of the root port, Device C calculates a designated port configuration BPDU for Port C1 (0, 9, 2, Port C1) and compares it with the existing configuration BPDU of Port C1 (0, 0, 0, Port A2). Device C finds that the existing configuration BPDU is superior to the calculated one and blocks Port C1 with the configuration BPDU unchanged. Then Port C1 does not forward data until a spanning tree calculation process is triggered by a new event, for example, the link between Device B and Device C is down.</td>
<td>Root port (Port C2): {0, 5, 1, Port B2}</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

In Table 5, each configuration BPDU contains the following fields: root bridge ID, root path cost, designated bridge ID, and designated port ID.

After the comparison processes described in Table 5, a spanning tree with Device A as the root bridge is established, and the topology is shown in Figure 11.
NOTE:
The spanning tree calculation process in this example is only simplified process.

The configuration BPDU forwarding mechanism of STP

The configuration BPDU of STP are forwarded following these guidelines:

- Upon network initiation, every router regards itself as the root bridge, generates configuration BPDU with itself as the root, and sends the configuration BPDU at a regular hello interval.
- If it is the root port that received a configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the router increases the message age carried in the configuration BPDU following a certain rule and starts a timer to time the configuration BPDU while sending out this configuration BPDU through the designated port.
- If the configuration BPDU received on a designated port has a lower priority than the configuration BPDU of the local port, the port immediately sends out its own configuration BPDU in response.
- If a path becomes faulty, the root port on this path no longer receives new configuration BPDU and the old configuration BPDU will be discarded due to timeout. The router generates a configuration BPDU with itself as the root and sends out 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, so 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 may occur.

STP timers

STP calculation involves the following timers: forward delay, hello time, and max age.

- Forward delay
  Forward delay is the delay time for state transition.
  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 right away, a temporary loop is likely to occur.
  For this reason, as a mechanism for state transition in STP, the newly elected root ports or designated ports require twice the forward delay time before transiting to the forwarding state to make sure that the new configuration BPDU has propagated throughout the network.

- Hello time
The router sends hello packets at the hello time interval to the neighboring routers to make sure that the paths are fault-free.

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

**RSTP**

Developed based on the 802.1w standard of IEEE, RSTP is an optimized version of STP. It achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP.

A newly elected RSTP root port rapidly enters the forwarding state if the old root port on the router has stopped forwarding data and the upstream designated port has started forwarding data.

A newly elected RSTP designated port rapidly enters the forwarding state if it is an edge port (which directly connects to a user terminal rather than to another router or a shared LAN segment) or it connects to a point-to-point link (to another router). Edge ports directly enter the forwarding state. Connecting to a point-to-point link, a designated port enters the forwarding state immediately after the router receives a handshake response from the directly connected router.

**MSTP**

**STP and RSTP limitations**

STP does not support rapid state transition of ports. A newly elected port must wait twice the forward delay time before transiting to the forwarding state, even if it connects to a point-to-point link or is an edge port.

Although RSTP supports rapid network convergence, it has the same drawback as STP—All bridges within a LAN share the same spanning tree, so redundant links cannot be blocked based on VLAN, and the packets of all VLANs are forwarded along the same spanning tree.

**MSTP features**

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

MSTP includes the following features:

- 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 divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a loop network into a loop-free tree, avoiding proliferation and endless cycling of packets in a loop network. In addition, it provides multiple redundant paths for data forwarding, supporting load balancing of VLAN data.
- MSTP is compatible with STP and RSTP.
MSTP basic concepts

Figure 12 shows a switched network that comprises four MST regions, each MST region comprising four MSTP devices. Figure 13 shows the networking topology of MST region 3. This section describes some basic concepts of MSTP.

Figure 12 Basic concepts in MSTP

MST region 1

MST region 2

MST region 3

MST region 4

VLAN 1 $\rightarrow$ MSTI 1
VLAN 2 $\rightarrow$ MSTI 2
Other VLANs $\rightarrow$ MSTI 0

VLAN 1 $\rightarrow$ MSTI 1
VLAN 2 $\rightarrow$ MSTI 2
Other VLANs $\rightarrow$ MSTI 0

VLAN 1 $\rightarrow$ MSTI 1
VLAN 2 & 3 $\rightarrow$ MSTI 2
Other VLANs $\rightarrow$ MSTI 0

VLAN 1 $\rightarrow$ MSTI 1
VLAN 2 & 3 $\rightarrow$ MSTI 2
Other VLANs $\rightarrow$ MSTI 0

CST

Figure 13 Network diagram and topology of MST region 3

To MST region 4

To MST region 2

Device A

Device B

Device C

Device D

VLAN 1 $\rightarrow$ MSTI 1
VLAN 2 & 3 $\rightarrow$ MSTI 2
Other VLANs $\rightarrow$ MSTI 0

MSTI 1

MSTI 2

MSTI 0

MSTI 0

Regional root

Topology of MSTIs in MST region 3
**MST region**

A multiple spanning tree region (MST region) consists of multiple routers in a switched network and the network segments among them. All these routers 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 routers to the same MST region. In Figure 12, the switched network comprises four MST regions, MST region 1 through MST region 4, and all routers in each MST region have the same MST region configuration.

**MSTI**

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

In Figure 13, MST region 3 comprises three MSTIs, MSTI 1, MSTI 2, and MSTI 0.

**VLAN-to-instance mapping table**

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

In Figure 13, the VLAN-to-instance mapping table of MST region 3 is: VLAN 1 to MSTI 1, VLAN 2 and VLAN 3 to MSTI 2, and 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 router, the CST is a spanning tree calculated by these routers through STP or RSTP.

The blue lines in Figure 12 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 12, 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 routers in a switched network. It consists of the ISTs in all MST regions and the CST.

In Figure 12, 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 may have different regional roots.
For example, in MST region 3 in Figure 13, the regional root of MSTI 1 is Device B, the regional root of MSTI 2 is Device C, and 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 12, for example, the common root bridge is a router in MST region 1.

**Port roles**

A port can play different roles in different MSTIs. As shown in Figure 14, an MST region comprises Device A, Device B, Device C, and Device D. Port A1 and port A2 of Device A connect to the common root bridge. Port B2 and Port B3 of Device B form a loop. Port C3 and Port C4 of Device C connect to other MST regions. Port D3 of Device D directly connects to a host.

**Figure 14 Port roles**

MSTP calculation involves these 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 router.
- **Alternate port**—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**—The backup port of a designated port. When the designated port is invalid, the backup port becomes the new designated port. When a loop occurs due to the interconnection of two ports of the same router running a spanning tree protocol, the router blocks either of the two ports, and the blocked port is the backup port.
- **Edge port**—An edge port does not connect to any network device or network segment, but directly connects to a user host.
- **Master port**—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 router. In MSTP calculation, a boundary port’s role on an MSTI is consistent with its role on the CIST. But 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 may 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 forwards 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 6** lists the port state(s) supported by each port role (“√” indicates that the port supports this state, and “—” indicates that the port does not support this state).

**Table 6** Port states supported by different port roles

<table>
<thead>
<tr>
<th>Port role (right)</th>
<th>Root port/master port</th>
<th>Designated port</th>
<th>Alternate port</th>
<th>Backup port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port state (below)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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 interconnected by a calculated CST. Inside an MST region, multiple spanning trees are calculated, each being an MSTI. Among these MSTIs, MSTI 0 is the IST. Similar to STP, MSTP uses configuration BPDUs to calculate spanning trees. The only difference between the two protocols is that an MSTP BPDU carries the MSTP configuration on the router from which this BPDU is sent.

**CIST calculation**

The calculation of a CIST tree is also the process of configuration BPDU comparison. During this process, the router with the highest priority is elected as the root bridge of the CIST. MSTP generates an IST within each MST region through calculation, and, at the same time, MSTP regards each MST region as a single router 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. MSTP performs a separate calculation process, which is similar to spanning tree calculation in STP, for each spanning tree. For more information, see “Calculation process of the STP algorithm.”
In MSTP, a VLAN packet is forwarded along the following paths:
- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

**Implementation of MSTP on routers**

MSTP is compatible with STP and RSTP. STP and RSTP protocol packets can be recognized by routers running MSTP and used for spanning tree calculation.

In addition to basic MSTP functions, the following functions are provided for ease of management:
- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU guard
- BPDU drop
- Support for hot swapping of interface cards and active/standby changeover.

**Protocols and standards**

The spanning tree protocols are documented in the following 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

**Spanning tree configuration task list**

Before configuring a spanning tree, you must determine the spanning tree protocol to be used (STP, RSTP, or MSTP) and plan the device roles (the root bridge or leaf node).

Complete the following tasks to configure STP:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Setting the spanning tree mode | Required  
Configuring the router to work in STP-compatible mode. |
<p>| Configuring the root bridge or a secondary root bridge | Optional |
| Configuring the device priority | Optional |
| Configuring the network diameter of a switched network | Optional |
| Configuring spanning tree timers | Optional |
| Configuring the timeout factor | Optional |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
<tr>
<td>Setting the spanning tree mode</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the router to work in STP-compatible mode.</td>
<td></td>
</tr>
<tr>
<td>Configuring the device priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the timeout factor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring path costs of ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuring the leaf nodes**

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the spanning tree mode</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the router to work in RSTP mode.</td>
<td></td>
</tr>
<tr>
<td>Configuring the VLAN Ignore feature</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring protection functions</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Complete the following tasks to configure RSTP:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the spanning tree mode</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the router to work in RSTP mode.</td>
<td></td>
</tr>
<tr>
<td>Configuring the root bridge</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the device priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the network diameter of a switched network</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring spanning tree timers</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the timeout factor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring edge ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port link type</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuring the root bridge**

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuring the leaf nodes**

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the spanning tree mode</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the router to work in RSTP mode.</td>
<td></td>
</tr>
</tbody>
</table>
### Task Remarks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the device priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the timeout factor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring edge ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring path costs of ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port link type</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
<tr>
<td>Performing mCheck</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the VLAN Ignore feature</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring protection functions</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Complete the following tasks to configure MSTP:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the spanning tree mode</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the router works in MSTP mode.</td>
<td></td>
</tr>
<tr>
<td>Configuring an MST region</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring the root bridge or a secondary root bridge</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the device priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum hops of an MST region</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the network diameter of a switched network</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring spanning tree timers</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the timeout factor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring edge ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port link type</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Configuring the root bridge

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the spanning tree mode</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the router works in MSTP mode.</td>
<td></td>
</tr>
<tr>
<td>Configuring an MST region</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Configuring the leaf nodes

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the spanning tree mode</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the router works in MSTP mode.</td>
<td></td>
</tr>
<tr>
<td>Configuring an MST region</td>
<td>Required</td>
</tr>
<tr>
<td>Task</td>
<td>Remarks</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Configuring the device priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the timeout factor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum port rate</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring edge ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring path costs of ports</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the port link type</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mode a port uses to recognize/send MSTP packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the spanning tree feature</td>
<td>Required</td>
</tr>
<tr>
<td>Performing mCheck</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the VLAN Ignore feature</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring Digest Snooping</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring No Agreement Check</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring protection functions</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**NOTE:**

- If GVRP and a spanning tree protocol are enabled on a router at the same time, GVRP packets are forwarded along the CIST. To advertise a certain VLAN within the network through GVRP, make sure that this VLAN is mapped to the CIST when you configure the VLAN-to-instance mapping table. For more information about GVRP, see the chapter “Configuring GVRP.”

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

- The spanning tree configurations made in system view take effect globally. Configurations made in Ethernet interface view take effect on the current interface only. Configurations made in port group view take effect on all member ports in the port group. 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 but not 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.

- Though the member ports of an aggregation group do not participate in spanning tree calculation, the ports still reserve its spanning tree configurations for participating spanning tree calculation after leaving the aggregation group.

### Configuring the spanning tree

#### Setting the spanning tree mode

The spanning tree modes include:
- **STP-compatible mode**—The router sends out STP BPDUs through all ports.
- **RSTP mode**—The router sends out RSTP BPDUs through all ports, and ports that connect to STP devices automatically transitions to the STP-compatible mode.
- **MSTP mode**—The router sends out MSTP BPDUs through all ports, and ports that connect to STP devices automatically transitions to the STP-compatible mode.

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 { stp</td>
</tr>
</tbody>
</table>

**Configuring an MST region**

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>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-list, 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>Display the MST region configurations that are not activated yet.</td>
<td>check region-configuration</td>
</tr>
<tr>
<td>7.</td>
<td>Activate MST region configuration manually.</td>
<td>active region-configuration</td>
</tr>
<tr>
<td>8.</td>
<td>Display the activated configuration information of the MST region.</td>
<td>display stp region-configuration [</td>
</tr>
</tbody>
</table>
NOTE:

- Two or more spanning tree devices belong to the same MST region only if they are configured to have the same format selector (0 by default, not configurable), MST region name, MST region revision level, and the same VLAN-to-instance mapping entries in the MST region, and they are interconnected via a physical link.

- The configuration of MST region-related parameters, especially the VLAN-to-instance mapping table, will result in a new spanning tree calculation. To reduce the possibility of topology instability, the MST region configuration takes effect only after you activate it by using the `active region-configuration` command, or enable a spanning tree protocol by using the `stp enable` command in the case that the spanning tree protocol is disabled.

### Configuring the root bridge or a secondary root bridge

The root bridge of a spanning tree is determined through spanning tree calculation. Alternatively, you can specify the router as the root bridge or a secondary root bridge.

A router 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, a router cannot be the root bridge and a secondary root bridge in the same spanning tree.

A spanning tree can have one root bridge only. If two or more routers are selected as the root bridge in a spanning tree at the same time, the router with the lowest MAC address wins out.

When the root bridge of an instance fails or is shut down, the secondary root bridge (if you have specified one) can take over the role of the primary root bridge. However, if you specify a new primary root bridge for the instance then, the secondary root bridge will not become the root bridge. If you have specified multiple secondary root bridges for an instance, when the root bridge fails, the secondary root bridge with the lowest MAC address is selected as the new root bridge.

#### Configuring the current router as the root bridge of a specific spanning tree

To configure the current router 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. system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>

2. Configure the current router as the root bridge.  
   - In STP/RSTP mode:  
     - `stp root primary`  
   - In MSTP mode:  
     - `stp [ instance instance-id ] root primary`

Use one of the commands. By default, a router does not function as the root bridge.

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

To configure the current router 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. system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Configuring the current router as a secondary root bridge

2. **Configure the current router as a secondary root bridge.**

   - **In STP/RSTP mode:**
     ```bash
stp root secondary
```
   - **In MSTP mode:**
     ```bash
stp [ instance instance-id ] root secondary
```

   Use one of the commands. By default, a router does not function as a secondary root bridge.

### Configuring the device priority

Device priorities participate in spanning tree calculation. The priority of a router determines whether the router can be elected as the root bridge of a spanning tree. A lower value indicates a higher priority. By setting the priority of a router to a low value, you can specify the router as the root bridge of the spanning tree. A spanning tree router can have different priorities in different MSTIs.

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

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

2. **Configure the priority of the current router.**

   - **In STP/RSTP mode:**
     ```bash
stp priority priority
```
   - **In MSTP mode:**
     ```bash
stp [ instance instance-id ] priority
```

   Use one of the commands. The default setting is 32768.

#### CAUTION:

- After configuring a router as the root bridge or a secondary root bridge, you cannot change the priority of the router.
- During root bridge selection, if all routers in a spanning tree have the same priority, the one with the lowest MAC address will be selected as the root bridge of the spanning tree.

### Configuring the maximum hops of an MST region

By setting the maximum hops of an MST region, you can restrict the region size. The maximum hops configured on the regional root bridge will be used as the maximum hops of the MST region.

The regional root bridge always sends a configuration BPDU with a hop count set to the maximum value. When a router receives this configuration BPDU, it decrements the hop count by 1 and uses the new hop count in the BPDUs it propagates. When the hop count of a BPDU reaches 0, it is discarded by the router that received it. Routers beyond the reach of the maximum hop can no longer take part in spanning tree calculation, and the size of the MST region is confined.
Make this configuration on the root bridge only. All the routers other than the root bridge in the MST region use the maximum hop value set for 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.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the maximum hops of the MST region.</td>
<td>stp max-hops hops</td>
</tr>
</tbody>
</table>

Configuring the network diameter of a switched network

Any two terminal devices in a switched network are interconnected through a specific path composed of a series of devices. The network diameter is the number of devices on the path composed of the most devices. The network diameter is a parameter that indicates the network size. A bigger network diameter indicates a larger network size.

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.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the network diameter of the switched network.</td>
<td>stp bridge-diameter diameter</td>
</tr>
</tbody>
</table>

NOTE:
- Based on the network diameter you configured, the system automatically sets an optimal hello time, forward delay, and max age for the router.
- Each MST region is considered as a router and the configured network diameter is effective only for the CIST (or the common root bridge), but not for MSTIs.

Configuring spanning tree timers

The following timers are used for spanning tree calculation:

- **Forward delay**
  It is the delay time for port state transition. To prevent temporary loops on a network, the spanning tree sets an intermediate port state, the learning state, before it transitions from the discarding state to the forwarding state, and requires that the port transitions its state after a forward delay timer to make sure that the state transition of the local port keeps synchronized with the peer.

- **Hello time**
  The router detects whether a link failure has occurred with the hello time interval. The spanning tree sends out a configuration BPDU every hello time interval. If the router receives no configuration BPDUs within the hello time interval, it recalculates the spanning tree.

- **Max age**
  In the CIST of an MSTP network, the router determines whether a configuration BPDU received by a port has expires based on the max age timer. If yes, a new spanning tree calculation process starts. The max age timer is ineffective for MSTIs.

To prevent network instability, make sure that the timer settings meet the following formulas:
- \(2 \times (\text{forward delay} - 1 \text{ second})/\text{max age}\)
- \(\text{Max age} \times 2 \times (\text{hello time} + 1 \text{ second})\)

H3C does not recommend you to manually set the spanning tree timers. Instead, you can specify the network diameter and let spanning tree protocols automatically calculate the timers based on the network diameter. If the network diameter uses the default value, the timers also use their default values.

Configure the timers on the root bridge only, and the timer settings on the root bridge apply to all the routers on the entire switched network.

To configure the spanning tree timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong></td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td><strong>2.</strong></td>
<td>Configure the forward delay timer.</td>
<td>stp timer forward-delay ( \text{time} )</td>
</tr>
<tr>
<td><strong>3.</strong></td>
<td>Configure the hello timer.</td>
<td>stp timer hello ( \text{time} )</td>
</tr>
<tr>
<td><strong>4.</strong></td>
<td>Configure the max age timer.</td>
<td>stp timer max-age ( \text{time} )</td>
</tr>
</tbody>
</table>

**NOTE:**
- The length of the forward delay timer is related to the network diameter of the switched network. The larger the network diameter is, the longer the forward delay time should be. If the forward delay timer is too short, temporary redundant paths may be introduced. If the forward delay timer is too long, it may take a long time for the network to converge. H3C recommends you to use the default setting.
- An appropriate hello time setting enables the router to timely detect link failures on the network without using excessive network resources. If the hello time is too long, the router will consider packet loss as a link failure and trigger a new spanning tree calculation process. If the hello time is too short, the router will frequently send the same configuration BPDUs, which add the router burden and waste network resources. H3C recommends you to use the default setting.
- If the max age timer is too short, the router will frequently launch spanning tree calculation and may consider network congestion as a link failure. If the max age timer is too long, the router may fail to timely detect link failures and launch spanning tree calculation, reducing the auto-sensing capability of the network. H3C recommends you to use the default setting.

**Configuring the timeout factor**

The timeout factor is a parameter used to decide the timeout time, as shown in the following formula:

\[
\text{Timeout time} = \text{timeout factor} \times 3 \times \text{hello time}.
\]

After the network topology is stabilized, each non-root-bridge router forwards configuration BPDUs to the downstream routers at the interval of hello time to check whether any link is faulty. If a router does not receive a BPDU from the upstream router within nine times the hello time, it assumes that the upstream router has failed and starts a new spanning tree calculation process.
Sometimes a router may fail to receive a BPDU from the upstream router because the upstream router is busy. If a spanning tree calculation occurs, the calculation can fail and also waste the network resources. In a stable network, you can prevent undesired spanning tree calculations by setting the timeout factor to 5, 6, or 7.

To configure the timeout factor:

<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 timeout factor of the router.</td>
<td>stp timer-factor factor</td>
</tr>
</tbody>
</table>

### Configuring the maximum port rate

The maximum rate of a port refers to the maximum number of BPDUs the port can send within each hello time. The maximum rate of a port is related to the physical status of the port and the network structure.

To configure the maximum rate of a port or a group of 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>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or port group view.</td>
<td>Interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the maximum rate of the ports.</td>
<td>stp transmit-limit limit</td>
</tr>
</tbody>
</table>

**NOTE:**
The higher the maximum port rate is, the more BPDUs will be sent within each hello time, and the more system resources will be used. By setting an appropriate maximum port rate, you can limit the rate at which the port sends BPDUs and prevent spanning tree protocols from using excessive network resources when the network becomes unstable. H3C recommends you to use the default setting.

### Configuring edge ports

If a port directly connects to a user terminal rather than another router or a shared LAN segment, this port is regarded as an edge port. When a network topology change occurs, an edge port will not cause a temporary loop. Because a router does not know whether a port is directly connected to a terminal, you need to manually configure the port to be an edge port. After that, this port can transition rapidly from the blocked state to the forwarding state without delay.

To specify a port or a group of ports as edge port or 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>system-view</td>
</tr>
</tbody>
</table>
Step | Command | Remarks |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter interface view or port group view.</td>
<td>Use one of the commands.</td>
</tr>
</tbody>
</table>
| | • Enter Ethernet interface view or Layer 2 aggregate interface view:  
interfacetype  
interface-number | | |
| | • Enter port group view:  
port-group manual  
port-group-name | | |
| 3. | Configure the current ports as edge ports. | By default, all ports are non-edge ports. |
| | stp edged-port enable | | |

**NOTE:**
- With BPDU guard disabled, when a port set as an edge port receives a BPDU from another port, it will become a non-edge port again. 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 transition to the forwarding state fast while ensuring network security.
- Among loop guard, root guard and edge port settings, only one function (whichever is configured the earliest) can take effect on a port at the same time.

### 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.

The router can automatically calculate the default path cost; alternatively, you can also configure the path cost for ports.

**Specifying a standard that the router uses when calculating the default path cost**

You can specify a standard for the router to use in automatic calculation for the default path cost. The router supports the following standards:
- **dot1d-1998**—The router calculates the default path cost for ports based on IEEE 802.1d-1998.
- **dot1t**—The router calculates the default path cost for ports based on IEEE 802.1t.
- **legacy**—The router calculates the default path cost for ports based on a private standard.

To specify a standard for the router to use when calculating 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>N/A</td>
</tr>
</tbody>
</table>
| 2. | Specify a standard for the router to use when calculating the default path costs of its ports. | Optional.  
The default setting is legacy. |
| | stp pathcost-standard  
{ dot1d-1998 | dot1t | legacy } | | |

⚠ **CAUTION:**

If you change the standard that the router uses in calculating the default path costs, you restore the path costs to the default.

Table 7 shows the mappings between the link speed and the path cost.
Table 7 Mappings between the link speed and the path cost

<table>
<thead>
<tr>
<th>Link speed</th>
<th>Port type</th>
<th>Path cost IEEE 802.1d-1998</th>
<th>Path cost IEEE 802.1t</th>
<th>Path cost Private standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N/A</td>
<td>65535</td>
<td>200,000,000</td>
<td>200,000</td>
</tr>
<tr>
<td></td>
<td>Single Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 2 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 3 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 4 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 2 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 3 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 4 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 2 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 3 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 4 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 2 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregate interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>containing 3 selected ports</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

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

**Configuring path costs of ports**

To configure the path cost of ports:
### Step 1: Enter system view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Step 2: Enter interface view or port group view.

- Enter Ethernet interface view or Layer 2 aggregate interface view:
  ```
  interface interface-type
  interface-number
  ```
- Enter port group view:
  ```
  port-group manual port-group-name
  ```

### Step 3: Configure the path cost of the ports.

- In STP/RSTP mode:
  ```
  stp cost cost
  ```
- In MSTP mode:
  ```
  stp [instance instance-id] cost cost
  ```

**NOTE:**

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

### Configuration example

```
# In MSTP mode, specify the router to calculate the default path costs of its ports by using IEEE 802.1d-1998, and set the path cost of GigabitEthernet 3/1/3 to 200 on MSTI 2.
<Sysname> system-view
<Sysname> stp pathcost-standard dot1d-1998
<Sysname> interface gigabitethernet 3/1/3
<Sysname-GigabitEthernet3/1/3> stp instance 2 cost 200
```

### Configuring the port priority

The priority of a port is an important factor in determining whether the port can be elected as the root port of a router. If all other conditions are the same, the port with the highest priority will be elected as the root port.

On a spanning tree router, a port can have different priorities and play different roles in different spanning trees, so that 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.

To configure the priority of a port or a group of ports:

<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>
### Configuring the port priority

In STP/RSTP mode:

```plaintext
stp port priority priority
```

In MSTP mode:

```plaintext
stp [ instance instance-id ] port priority priority
```

Use one of the commands.

The default setting is 128.

---

### 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 transition to the forwarding state after a proposal-agreement handshake process.

To configure the link type of a port or a group of ports:

<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 Ethernet interface view or Layer 2 aggregate interface view:  
      | interface interface-type interface-number | Use one of the commands. |
|      | Enter port group view:  
      | port-group manual port-group-name | |
|      | stp point-to-point { auto | force-false | force-true } | By default, the link type is auto where the port automatically detects the link type. |

**NOTE:**
- You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that works in full duplex mode. H3C recommends you to use the default setting and let the router to automatically detect the port link type.
- The `stp point-to-point force-false` or `stp point-to-point force-true` command configured on a port in MSTP mode is effective for all MSTIs.
- If the physical link to which the port connects is not a point-to-point link but you set it to be one, the configuration may bring a temporary loop.
Configuring the mode a port uses to recognize/send MSTP packets

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

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

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

You can configure the MSTP packet format on a port. When working in MSTP mode after the configuration, the port sends and receives only MSTP packets of the format you have configured to communicate with routers that send packets of the same format.

To configure the MSTP packet format to be supported on a port or a group of 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>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or port group view.</td>
<td>Use one of the commands.</td>
</tr>
<tr>
<td></td>
<td>• Enter Ethernet interface view or Layer 2 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the mode the port uses to recognize/send MSTP packets.</td>
<td>stp compliance { auto</td>
</tr>
</tbody>
</table>

**NOTE:**

- MSTP provides the MSTP packet format incompatibility guard function. In MSTP mode, if a port is configured to recognize/send MSTP packets in a mode other than **auto**, and receives a packet in a format different from the specified type, the port will become a designated port and remain in the discarding state to prevent the occurrence of a loop.
- MSTP provides the MSTP packet format frequent change guard function. If a port receives MSTP packets of different formats frequently, the MSTP packet format configuration contains errors. If the port is working in MSTP mode, it will be shut down for protection. The closed ports can be reactivated after a detection interval. For more information about the detection interval, see Fundamentals Configuration Guide.

Enabling the spanning tree feature

You must enable the spanning tree feature for the router before any other spanning tree related configurations can take effect.

To enable the spanning tree feature:
Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
2. | Enable the spanning tree feature globally. | stp enable | By default, the spanning tree feature is disabled.
3. | Enter interface view or port group view. | interface interface-type interface-number | Use either command.
4. | Enable the spanning tree feature for the port or group of ports. | stp enable | Optional. By default, the spanning tree feature is enabled for all ports.

**NOTE:**
You can disable the spanning tree feature for certain ports with the `undo stp enable` command to exclude them from spanning tree calculation and save CPU resources of the router. However, use this command with caution because the ports with the spanning tree feature disabled will keep forwarding data traffic and discard STP BPDUs, and loops can occur.

### Performing mCheck

If a port on a router running MSTP or RSTP connects to an STP router, this port will automatically transition to the STP-compatible mode. However, it cannot automatically transition back to the original mode when:

- The STP router is shut down or removed.
- The STP router transitions to the MSTP or RSTP mode.

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

You can perform mCheck on a port through the following two approaches, which lead to the same result.

#### Performing mCheck globally

To perform global mCheck:

<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>Perform mCheck.</td>
</tr>
</tbody>
</table>

#### Performing mCheck in interface view

To perform 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>
</tbody>
</table>
Step Command Remarks
1. Enter system view. system-view N/A
2. Enable VLAN Ignore for the specified VLANs. stp ignored vlan vlan-list By default, VLAN Ignore is disabled.
3. Display VLAN Ignore-enabled VLANs. display stp ignored-vlan [ | { begin | exclude | include } regular-expression ] Optional. Available in any view

VLAN Ignore configuration example

1. Network requirements

Configuring the VLAN Ignore feature

Traffic of a VLAN on a complex network may be blocked by the spanning tree.

Figure 15 VLAN connectivity blocked by MSTP

As shown in Figure 15:

- Port A1 on Device A allows the traffic of VLAN 1 to pass through, and Port A2 allows the traffic of VLAN 2 to pass through.
- Port B1 on Device B allows the traffic of VLAN 1 to pass through, and Port B2 allows the traffic of VLAN 2 to pass through.
- Device A and Device B run a spanning tree protocol. Device A is the root bridge, and Port A1 and Port A2 are designated ports. On Device B, Port B1 is the root port, and port B2 is the blocked port. Traffic of VLAN 2 is blocked.
- Enabling the VLAN Ignore feature for a VLAN can make ports of the VLAN forward packets normally rather than comply with the spanning tree calculation result.
As shown in Figure 16:

- Device A and Device B are directly connected.
- GigabitEthernet 3/1/1 on Device A and GigabitEthernet 3/1/1 on Device B allow the traffic of VLAN 1 to pass through. GigabitEthernet 3/1/2 on Device A and GigabitEthernet 3/1/2 on Device B allow the traffic of VLAN 2 to pass through.
- Device A is the root bridge, and Device A and Device B both run a spanning tree protocol. GigabitEthernet 3/1/2 on Device B is blocked, causing traffic of VLAN 2 to be blocked.

Configure VLAN Ignore to keep GigabitEthernet 3/1/2 of Device B in the forwarding state.

**Figure 16 Network diagram**

![Network diagram]

2. Configuration procedure

   # Enable VLAN Ignore for VLAN 2 on Device B.
   <DeviceB> system-view
   [DeviceB] stp ignored vlan 2

   # Display the VLAN Ignore-enabled VLAN.
   [DeviceB] display stp ignored-vlan
   STP-Ignored VLAN: 2

### Configuring Digest Snooping

As defined in IEEE 802.1s, interconnected devices are in the same region only when the MST region-related configurations (region name, revision level, VLAN-to-instance mappings) on them are identical. A spanning tree device identifies devices in the same MST region by checking the configuration ID in BPDU packets. The configuration ID includes the region name, revision level, configuration digest that is in 16-byte length and is the result calculated via the HMAC-MD5 algorithm based on VLAN-to-instance mappings.

Spanning tree implementations vary with vendors, and the configuration digests calculated using private keys is different. As a result, devices of different vendors in the same MST region cannot communicate with each other.

To enable communication between an H3C router and a third-party device, enable the Digest Snooping feature on the port connecting the H3C router to the third-party device in the same MST region.

---

**NOTE:**

Before enabling Digest Snooping, make sure that associated devices of different vendors are connected and run spanning tree protocols.
Configuring the Digest Snooping feature

You can enable Digest Snooping only on the H3C router that 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 interface view or port group view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter Ethernet interface view or Layer 2 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Enable Digest Snooping on the interface or port group.</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 global Digest Snooping.</td>
<td>stp config-digest-snooping</td>
</tr>
</tbody>
</table>

⚠️ CAUTION:
- With the Digest Snooping feature enabled, comparison of configuration digest is not needed for in-the-same-region check, so the VLAN-to-instance mappings must be the same on associated ports.
- With global Digest Snooping enabled, modification of VLAN-to-instance mappings and removing of the current region configuration using the undo stp region-configuration command are not allowed. You can only modify the region name and revision level.
- You must enable Digest Snooping both globally and on associated ports to make it take effect. To make the configuration effective on all configured ports and while reducing impact on the network, enable Digest Snooping on all associated ports first and then globally.
- To prevent loops, do not enable Digest Snooping on MST region edge ports.
- H3C recommends you to enable Digest Snooping first and then the spanning tree feature. To avoid traffic interruption, do not configure Digest Snooping when the network works well.

Digest Snooping configuration example

1. Network requirements
   As shown in Figure 17, 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 Device A’s and Device B’s ports that connect to Device C, so that the three devices can communicate with one another.
2. Configuration procedure

# Enable Digest Snooping on GigabitEthernet 3/1/1 of Device A and enable global Digest Snooping on Device A.

```plaintext
<DeviceA> system-view
[DeviceA] interface gigabitethernet 3/1/1
[DeviceA-GigabitEthernet3/1/1] stp config-digest-snooping
[DeviceA-GigabitEthernet3/1/1] quit
[DeviceA] stp config-digest-snooping
```

# Enable Digest Snooping on GigabitEthernet 3/1/1 of Device B and enable global Digest Snooping on Device B.

```plaintext
<DeviceB> system-view
[DeviceB] interface gigabitethernet 3/1/1
[DeviceB-GigabitEthernet3/1/1] stp config-digest-snooping
[DeviceB-GigabitEthernet3/1/1] quit
[DeviceB] stp 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 downstream device’s root port sends an agreement packet only after it receives an agreement packet from the upstream device.
- For RSTP, the downstream device sends an agreement packet regardless of whether an agreement packet from the upstream device is received.

Figure 18 shows the rapid state transition mechanism on MSTP designated ports.
Figure 18 Rapid state transition of an MSTP designated port

If the upstream device is a third-party device, the rapid state transition implementation may be limited. For example, when the upstream device uses a rapid transition mechanism similar to that of RSTP, and the downstream device adopts MSTP and does not work in RSTP mode, the root port on the downstream device receives no agreement packet from the upstream device and sends no agreement packets to the upstream device. As a result, the designated port of the upstream device fails to transit rapidly and can only change to the forwarding state after a period twice the Forward Delay.

You can enable the No Agreement Check feature on the downstream device’s port to enable the designated port of the upstream device to transit its state rapidly.

Configuration Prerequisites

Before you configure the No Agreement Check function, complete the following tasks:

- Connect a router to a third-party upstream router supporting spanning tree protocols via a point-to-point link.
- Configure the same region name, revision level and VLAN-to-instance mappings on the two routers, assigning them to the same region.

Configuring the No Agreement Check function

To make the No Agreement Check feature take effect, enable it 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 interface view or port group view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter Ethernet interface view or layer 2 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-group manual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-group-name</td>
<td></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**

1. **Network requirements**
   As shown in Figure 20:
   - Device A connects to Device B, a third-party device that has a different spanning tree implementation. Both devices are in the same region.
   - Device B is the regional root bridge, and Device A is the downstream device.

   **Figure 20 Network diagram**

2. **Configuration procedure**
   # Enable No Agreement Check on GigabitEthernet 3/1/1 of Device A.
   ```
   <DeviceA> system-view
   [DeviceA] interface gigabitethernet 3/1/1
   [DeviceA-GigabitEthernet3/1/1] stp no-agreement-check
   ```

**Configuring protection functions**

A spanning tree device supports the following protection functions:
- BPDU guard
- Root guard
- Loop guard
- TC-BPDU guard

**Configuration prerequisites**

The spanning tree feature has been correctly configured on the router.
Enabling BPDU guard

For access layer devices, the access ports can directly connect to the user terminals (such as PCs) or file servers. The access ports are configured as edge ports to allow rapid transition. When these ports receive configuration BPDU, the system will automatically set these ports as non-edge ports and start a new spanning tree calculation process. This will cause a change of network topology. Under normal conditions, these ports should not receive configuration BPDU. However, if someone forges configuration BPDU maliciously to attack the devices, the network will become instable.

The spanning tree protocol provides the BPDU guard function to protect the system against such attacks. With the BPDU guard function enabled on the routers, when edge ports receive configuration BPDU, the system will close these ports and notify the NMS that these ports have been closed by the spanning tree protocol. The closed ports will be re-activated by the router after a detection interval. For more information about this detection interval, see Fundamentals Configuration Guide.

Make this configuration on a router with edge ports configured.

To enable 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>Enable the BPDU guard function for the router.</td>
<td>stp bpdu-protection</td>
</tr>
</tbody>
</table>

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

Enabling root guard

**NOTE:**
H3C recommends you to enable 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 may receive a configuration BPDU with a higher priority. The current legal root bridge will be superseded by another router, causing an undesired change of the network topology. As a result, the traffic that should go over high-speed links is switched to low-speed links, resulting in network congestion.

To prevent this situation from happening, MSTP provides the root guard function. If the root guard function is enabled on a port of a root bridge, this port will keep playing the role of designated port on all MSTIs. Once this port receives a configuration BPDU with a higher priority from an MSTI, it immediately sets that port to the listening state in the MSTI, without forwarding the packet (this is equivalent to disconnecting the link connected with this port in the MSTI). If the port receives no BPDU with a higher priority within twice the forwarding delay, it will revert to its original state.

Make this configuration on a designated port.

To enable root guard:
Step | Command | Remarks
--- | --- | ---
1. Enter system view. | system-view | N/A

2. Enter interface view or port group view.
   - Enter Ethernet interface view or Layer 2 aggregate interface view:
     ```
     interface interface-type
     interface-number
     ```
   - Enter port group view:
     ```
     port-group manual
     port-group-name
     ```
   Use either command.

3. Enable the root guard function for the port(s).
   ```
   stp root-protection
   ```
   By default, root guard is disabled.

NOTE:
Among loop guard, root guard and edge port settings, only one function (whichever is configured the earliest) can take effect on a port at the same time.

Enabling loop guard

By keeping receiving BPDUs from the upstream device, a router can maintain the state of the root port and blocked ports. However, due to link congestion or unidirectional link failures, these ports may fail to receive BPDUs from the upstream devices. The router will reselect the port roles: Those ports in forwarding state that failed to receive upstream BPDUs will become designated ports, and the blocked ports will transition to the forwarding state, resulting in loops in the switched network. The loop guard function can suppress the occurrence of such loops.

The initial state of a loop guard-enabled port is discarding in every MSTI. When the port receives BPDUs, its state transitions normally. Otherwise, it stays in the discarding state to prevent temporary loops.

Make this configuration on the root port and alternate ports of a router.

To enable loop guard:

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

2. Enter interface view or port group view.
   - Enter Ethernet interface view or Layer 2 aggregate interface view:
     ```
     interface interface-type
     interface-number
     ```
   - Enter port group view:
     ```
     port-group manual
     port-group-name
     ```
   Use either command.

3. Enable the loop guard function for the ports.
   ```
   stp loop-protection
   ```
   By default, loop guard is disabled.
NOTE:
- Do not enable loop guard on a port connecting user terminals. Otherwise, the port will stay in the discarding state in all MSTIs because it cannot receive BPDUs.
- Among loop guard, root guard and edge port settings, only one function (whichever is configured the earliest) can take effect on a port at the same time.

Enabling TC-BPDU guard

When receiving topology change (TC) BPDUs (the BPDUs used to notify topology changes), a router flushes its forwarding address entries. If someone forges TC-BPDUs to attack the router, the router will receive a large number of TC-BPDUs within a short time and be busy with forwarding address entry flushing. This affects network stability.

With the TC-BPDU guard function, you can set the maximum number of immediate forwarding address entry flushes that the router can perform every a certain period of time (10 seconds). For TC-BPDUs received in excess of the limit, the router performs forwarding address entry flush when the time period expires. This prevents frequent flushing of forwarding address entries.

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>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the TC-BPDU guard function.</td>
<td>stp tc-protection enable</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the maximum number of forwarding address entry flushes that the router can perform every 10 seconds.</td>
<td>stp tc-protection threshold number</td>
</tr>
</tbody>
</table>

NOTE:
H3C does not recommend you disable this feature.

Displaying and maintaining the spanning tree

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about ports blocked by spanning tree protection functions.</td>
<td>display stp abnormal-port</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display BPDU statistics on ports.</td>
<td>display stp bpdu-statistics interface interface-type interface-number</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display information about ports shut down by spanning tree protection functions.</td>
<td>display stp down-port</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the historical information of port role calculation for the specified MSTI or all MSTIs.</td>
<td>display stp [ instance instance-id ] history [ slot slot-number ]</td>
<td>Available in any view</td>
</tr>
</tbody>
</table>
**MSTP configuration example**

**Network requirements**

As shown in Figure 21, all devices on the network are in the same MST region, Device A and Device B work at the distribution layer, and Device C and Device D work at the access layer.

Configure MSTP so that packets of different VLANs are forwarded along different spanning trees: Packets of VLAN 10 are forwarded along MSTI 1, those of VLAN 30 are forwarded along MSTI 3, those of VLAN 40 are forwarded along MSTI 4, and those of VLAN 20 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, so the root bridges of MSTI 1 and MSTI 3 are Device A and Device B respectively, and the root bridge of MSTI 4 is Device C.

**Figure 21 Network diagram**
Configuration procedure

1. Configure VLANs and VLAN member ports. (Details not shown)
   Create VLAN 10, VLAN 20, and VLAN 30 on Device A and Device B respectively, VLAN 10, VLAN 20, and VLAN 40 on Device C, and 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, configure the MST region name as `example`, map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4 respectively, and configure the revision level of the MST region as 0.
   <DeviceA> system-view
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] region-name example
   [DeviceA-mst-region] instance 1 vlan 10
   [DeviceA-mst-region] instance 3 vlan 30
   [DeviceA-mst-region] instance 4 vlan 40
   [DeviceA-mst-region] revision-level 0
   
   # Activate MST region configuration.
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   
   # Specify the current device as the root bridge of MSTI 1.
   [DeviceA] stp instance 1 root primary
   
   # Enable the spanning tree feature globally.
   [DeviceA] stp enable

3. Configure Device B:
   
   # Enter MST region view, configure the MST region name as `example`, map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4 respectively, and configure the revision level of the MST region as 0.
   <DeviceB> system-view
   [DeviceB] stp region-configuration
   [DeviceB-mst-region] region-name example
   [DeviceB-mst-region] instance 1 vlan 10
   [DeviceB-mst-region] instance 3 vlan 30
   [DeviceB-mst-region] instance 4 vlan 40
   [DeviceB-mst-region] revision-level 0
   
   # Activate MST region configuration.
   [DeviceB-mst-region] active region-configuration
   [DeviceB-mst-region] quit
   
   # Specify the current device as the root bridge of MSTI 3.
   [DeviceB] stp instance 3 root primary
   
   # Enable the spanning tree feature globally.
   [DeviceB] stp enable

4. Configure Device C:
   
   # Enter MST region view, configure the MST region name as `example`, map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4 respectively, and configure the revision level of the MST region as 0.
Configure Device C:

# Enter MST region view, configure the MST region name as example, map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4 respectively, and configure the revision level of the MST region as 0.

<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
[DeviceC-mst-region] revision-level 0

# Activate MST region configuration.
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit

# Specify the current device as the root bridge of MSTI 4.
[DeviceC] stp instance 4 root primary

# Enable the spanning tree feature globally.
[DeviceC] stp enable

5. Configure Device D:

# Enter MST region view, configure the MST region name as example, map VLAN 10, VLAN 30, and VLAN 40 to MSTI 1, MSTI 3, and MSTI 4 respectively, and configure the revision level of the MST region as 0.

<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
[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 enable

6. Verify the configurations:

You can use the `display stp brief` command to display brief spanning tree information on each device after the network is stable.

# Display brief spanning tree information on Device A.

[DeviceA] display stp brief

<table>
<thead>
<tr>
<th>MSTID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/1</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/3</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>GigabitEthernet4/1/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>GigabitEthernet4/1/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet4/1/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet4/1/3</td>
<td>ROOT</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>MSTID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/1</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/3</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>GigabitEthernet4/1/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>GigabitEthernet4/1/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet4/1/2</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet4/1/3</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
</tbody>
</table>
0  GigabitEthernet4/1/1    DESI  FORWARDING    NONE
0  GigabitEthernet4/1/2    DESI  FORWARDING    NONE
0  GigabitEthernet4/1/3    DESI  FORWARDING    NONE
1  GigabitEthernet4/1/2    DESI  FORWARDING    NONE
1  GigabitEthernet4/1/3    ROOT  FORWARDING    NONE
3  GigabitEthernet4/1/1    DESI  FORWARDING    NONE
3  GigabitEthernet4/1/3    DESI  FORWARDING    NONE

# Display brief spanning tree information on Device C.
[DeviceC] display stp brief

<table>
<thead>
<tr>
<th>MSTID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/1</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/2</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/3</td>
<td>DESI</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>GigabitEthernet4/1/1</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>GigabitEthernet4/1/2</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>4</td>
<td>GigabitEthernet4/1/3</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>MSTID</th>
<th>Port</th>
<th>Role</th>
<th>STP State</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/1</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/2</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>0</td>
<td>GigabitEthernet4/1/3</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet4/1/1</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet4/1/2</td>
<td>ALTE</td>
<td>DISCARDING</td>
<td>NONE</td>
</tr>
<tr>
<td>4</td>
<td>GigabitEthernet4/1/3</td>
<td>ROOT</td>
<td>FORWARDING</td>
<td>NONE</td>
</tr>
</tbody>
</table>

Based on the output, you can draw the MSTI mapped to each VLAN, as shown in Figure 22.

Figure 22 MSTIs mapped to different VLANs

MSTI mapped VLAN 10  
MSTI mapped to VLAN 20

MSTI mapped to VLAN 30  
MSTI mapped to VLAN 40

Root device  
Normal link  
Blocked link
Configuring Ethernet link aggregation

NOTE:
In this documentation, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E.

Overview

Ethernet link aggregation, or simply link aggregation, combines multiple physical Ethernet ports into one logical link, called an aggregate link. Link aggregation delivers the following benefits:

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

As shown in Figure 23, Device A and Device B are connected by three physical Ethernet links. These physical Ethernet links are combined into an aggregate link, link aggregation 1. The bandwidth of this aggregate link is as high as the total bandwidth of these three physical Ethernet links. At the same time, the three Ethernet links back up one another.

Figure 23 Diagram for Ethernet link aggregation

Basic concepts

Aggregation group, member port, and aggregate interface

Link aggregation is implemented through link aggregation groups. An aggregation group is a group of Ethernet interfaces combined together, which are called member ports of the aggregation group. For each aggregation group, a logical interface, called an aggregate interface, is created. To an upper layer entity that uses the link aggregation service, a link aggregation group looks like a single logical link and data traffic is transmitted through the aggregate interface.

Aggregate interfaces have the following types: bridge-aggregation (BAGG) interfaces, also called Layer 2 aggregate interfaces, and route-aggregation (RAGG) interfaces, also called Layer 3 aggregate interfaces. When you create an aggregate interface, the router automatically creates an aggregation group of the same type and number as the aggregate interface. For example, when you create interface Bridge-Aggregation 1, Layer 2 aggregation group 1 is created.

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

- The router supports up to 240 aggregation groups.
- On a Layer 3 aggregate interface, you can create subinterfaces. These subinterfaces are logical interfaces that operate at the network layer. They can receive VLAN tagged packets for their Layer 3 aggregate interface.
- The rate of an aggregate interface equals the total rate of its member ports in Selected state, and its duplex mode is the same as the selected member ports. For more information about the states of member ports in an aggregation group, see “Aggregation states of member ports in an aggregation group.”

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

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

- **Selected**—A Selected port can forward user traffic.
- **Unselected**—An Unselected port cannot forward user traffic.

### Operational key

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

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

### Configuration classes

Every configuration setting on a port may affect its aggregation state. Port configurations fall into the following classes:

- **Port attribute configurations**, including port rate, duplex mode, and link status (up/down), which are the most basic port configurations.
- **Class-two configurations**, as described in Table 8. A member port can be placed in Selected state only if it has the same class-two configurations as the aggregate interface.

#### Table 8 Class-two configurations

<table>
<thead>
<tr>
<th>Feature</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port isolation</td>
<td>Whether the port has joined an isolation group, and the isolation group to which the port belongs</td>
</tr>
<tr>
<td>QinQ</td>
<td>QinQ enable state (enable/disable), TPID for VLAN tags, outer VLAN tags to be added, inner-to-outer VLAN priority mappings, inner-to-outer VLAN tag mappings, inner VLAN ID substitution mappings</td>
</tr>
<tr>
<td>VLAN</td>
<td>Permitted VLAN IDs, PVID, link type (trunk, hybrid, or access), IP subnet-based VLAN configuration, protocol-based VLAN configuration, VLAN tagging mode</td>
</tr>
<tr>
<td>MAC address learning</td>
<td>MAC address learning capability, MAC address learning limit, forwarding of frames with unknown destination MAC addresses after the MAC address learning limit is reached</td>
</tr>
</tbody>
</table>
NOTE:

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

- Any class-two configuration change may affect the aggregation state of link aggregation member ports and ongoing traffic. To make sure that you are aware of the risk, the system displays a warning message every time you attempt to change a class-two configuration setting on a member port.

- Class-one configurations do not affect the aggregation state of the member port even if they are different from those on the aggregate interface. GVRP and MSTP settings are examples of class-one configurations.

NOTE:
The class-one configuration for a member port is effective only when the member port leaves the aggregation group.

Reference port

When setting the aggregation state of the ports in an aggregation group, the system automatically picks a member port as the reference port. A Selected port must have the same port attributes and class-two configurations as the reference port.

LACP

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables dynamic aggregation of physical links. It uses link aggregation control protocol data units (LACPDUs) for exchanging aggregation information between LACP-enabled devices.

1. LACP functions

   The IEEE 802.3ad LACP offers basic LACP functions and extended LACP functions, as described in Table 9.

Table 9 Basic and extended LACP functions

<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 system LACP priority, system MAC address, port aggregation priority, port number, and operational key. Each member port in a LACP-enabled aggregation group exchanges information with its peer. When a member port receives an LACPDU, it compares the received information with the information received on the other member ports. In this way the two systems reach an agreement on which ports should be placed in Selected state.</td>
</tr>
</tbody>
</table>
| Extended LACP functions | Implemented by extending the LACPDU with new Type/Length/Value (TLV) fields. This is how the LACP multi-active detection (MAD) mechanism of the Intelligent Resilient Framework (IRF) feature is implemented.  
   - If a device supports both LACP extensions and IRF, it can participate in LACP MAD either as an IRF member device or an intermediate device.  
   - If a device supports LACP extensions but not IRF, it can participate in LACP MAD only as an intermediate device. |

NOTE:
The SR8800 routers do not support IRF.
2. LACP priorities

LACP priorities have the following types: system LACP priority and port aggregation priority, as described in Table 10.

Table 10 LACP priorities

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Remarks</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.</td>
<td>The smaller the priority value, the higher the priority.</td>
</tr>
<tr>
<td></td>
<td>In dynamic link aggregation, the system that has higher system LACP priority sets the Selected state of member ports on its side first and then the system that has lower priority sets port state accordingly.</td>
<td></td>
</tr>
<tr>
<td>Port aggregation priority</td>
<td>Determines the likelihood of a member port to be selected on a system.</td>
<td>The higher port aggregation priority, the higher likelihood.</td>
</tr>
<tr>
<td></td>
<td>The higher port aggregation priority, the higher likelihood.</td>
<td></td>
</tr>
</tbody>
</table>

3. 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 fails to receive LACPDUs from the peer within three times the LACP timeout interval, the member port assumes that the peer port has failed. You can configure the LACP timeout interval as the short timeout interval (1 second) or the long timeout interval (30 seconds).

Link aggregation modes

Link aggregation has the following modes: dynamic and static. Dynamic link aggregation uses LACP and static link aggregation does not. Table 11 compares the two aggregation modes.

Table 11 A comparison between static and dynamic aggregation modes

<table>
<thead>
<tr>
<th>Aggregation mode</th>
<th>LACP status on member ports</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>Disabled</td>
<td></td>
<td>Aggregation is stable. The aggregation state of the member ports are not affected by the peer ports.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>Enabled</td>
<td></td>
<td>The administrator does not need to maintain link aggregations. The peer systems maintain the aggregation state of the member ports automatically.</td>
</tr>
</tbody>
</table>

In a dynamic link aggregation group:
- A Selected port can receive and send LACPDUs.
- An Unselected port can receive and send LACPDUs only if it is up and has the same class-two configurations as the aggregate interface.

Aggregating links in static mode

LACP is disabled on the member ports in a static aggregation group. You must manually maintain the aggregation state of the member ports.
The static link aggregation procedure comprises:

- Selecting a reference port
- Setting the aggregation state of each member port

**Selecting a reference port**

The system selects a reference port from the member ports that are in the up state and have the same class-two configurations as the aggregate interface.

The candidate ports are sorted by aggregation priority, duplex, and speed in this order: lowest aggregation priority value, full duplex/high speed, full duplex/low speed, half duplex/high speed, and half duplex/low speed. The one at the top is selected as the reference port. If two ports have the same aggregation priority, duplex mode, and speed, the one with the lower port number wins out.

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

After selecting the reference port, the static aggregation group sets the aggregation state of each member port, as shown in Figure 24.

**Figure 24 Setting the aggregation state of a member port in a static aggregation group**

<table>
<thead>
<tr>
<th>Port attribute/class 2 configurations same as the reference port?</th>
<th>Port number as low as to set the port in the Selected state?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Is there any hardware restriction?</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the port up?</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:**

- To ensure stable aggregation state and service continuity, do not change port attributes or class-two configurations on any member port.
- If a static aggregation group has reached the limit on Selected ports, any port joins the group is placed in Unselected state to avoid traffic interruption on the current Selected ports. Avoid this situation, however, because it may cause the aggregation state of a port to change after a reboot.

71
Aggregating links in dynamic mode

LACP is automatically enabled on all member ports in a dynamic aggregation group. The protocol automatically maintains the aggregation state of ports.

The dynamic link aggregation procedure comprises:

- Selecting a reference port
- Setting the aggregation state of each member port

Selecting a reference port

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

1. Compare the system ID (comprising the system LACP priority and the system MAC address). The system with the lower LACP priority value wins out. If they are the same, compare the system MAC addresses. The system with the lower MAC address wins.

2. The system with the smaller system ID selects the port with the smallest port ID as the reference port. A port ID comprises a port aggregation priority and a port number. The port with the lower aggregation priority value wins out. If two ports have the same aggregation priority, the system compares their port numbers. The port with the smaller port number wins.

Setting the aggregation state of each member port

After the reference port is selected, the system with the lower system ID sets the state of each member port in the dynamic aggregation group on its side as shown in Figure 25.
Meanwhile, the system with the higher system ID, being aware of the aggregation state changes on the remote system, sets the aggregation state of local member ports the same as their peer ports.

**NOTE:**
- A dynamic link aggregation group preferably sets full-duplex ports as the Selected ports, and will set one, and only one, half-duplex port as a Selected port when none of the full-duplex ports can be selected or only half-duplex ports exist in the group.
- To ensure stable aggregation state and service continuity, do not change port attributes or class-two configurations on any member port.
- In a dynamic aggregation group, when the aggregation state of a local port changes, the aggregation state of the peer port also changes.
- A port that joins a dynamic aggregation group after the Selected port limit has been reached is placed in Selected state if it is more eligible for being selected than a current member port.
Load sharing criteria for link aggregation groups

In a link aggregation group, traffic may be load-shared across the selected member ports based on a set of criteria, depending on your configuration.

You can choose one of the following criteria or any combination for load sharing:

- MAC addresses
- IP addresses
- Service port numbers
- Ingress ports
- MPLS labels

Ethernet link aggregation configuration task list

Complete the following tasks to configure Ethernet link aggregation:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an aggregation group</td>
<td>Select either task</td>
</tr>
<tr>
<td>Configuring a static aggregation group</td>
<td></td>
</tr>
<tr>
<td>Configuring a dynamic aggregation group</td>
<td></td>
</tr>
<tr>
<td>Configuring the description of an aggregate interface or subinterface</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the MTU of a Layer 3 aggregate interface or subinterface</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling link state traps for an aggregate interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Setting the minimum number of Selected ports for an aggregation group</td>
<td>Optional</td>
</tr>
<tr>
<td>Shutting down an aggregate interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Restoring the default settings for an aggregate interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring load sharing criteria for link aggregation groups</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Configuring an aggregation group

You can choose to create a Layer 2 or Layer 3 link aggregation group depending on the ports to be aggregated:

- To aggregate Layer 2 Ethernet interfaces, create a Layer 2 link aggregation group.
- To aggregate Layer 3 Ethernet interfaces, create a Layer 3 link aggregation group.

Configuration guidelines

You cannot assign a port to a Layer 2 aggregation group if any of the features listed in Table 12 is configured on the port.
### Table 12 Features incompatible with Layer 2 aggregation groups

<table>
<thead>
<tr>
<th>Feature</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet filtering</td>
<td>Packet-filter firewall in Security Configuration Guide</td>
</tr>
<tr>
<td>Ethernet frame filtering</td>
<td>Packet-filter firewall in Security Configuration Guide</td>
</tr>
<tr>
<td>IP source guard</td>
<td>IP source guard in Security Configuration Guide</td>
</tr>
<tr>
<td>802.1X</td>
<td>802.1X in Security Configuration Guide</td>
</tr>
<tr>
<td>Ports specified as source interfaces in portal-free rules</td>
<td>Portal in Security Configuration Guide</td>
</tr>
</tbody>
</table>

You cannot assign a port to a Layer 3 aggregation group if any of the features listed in Table 13 is configured on the port.

### Table 13 Interfaces that cannot be assigned to a Layer 3 aggregation group

<table>
<thead>
<tr>
<th>Interface type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces configured with IP addresses</td>
<td>IP addressing in Layer 3—IP Services Configuration Guide</td>
</tr>
<tr>
<td>Interfaces configured as DHCP/BOOTP clients</td>
<td>DHCP in Layer 3—IP Services Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>VRRP in High Availability Configuration Guide</td>
</tr>
<tr>
<td>Portal</td>
<td>Portal in Security Configuration Guide</td>
</tr>
</tbody>
</table>

⚠️ **CAUTION:**

- Do not configure any Layer 3 features, such as MPLS and VPN, on a port to be added to a Layer 3 aggregation group. Remove any Layer 3 feature configured on a port before adding it to a Layer 3 aggregation group.

- After adding a port to a Layer 3 aggregation group, configure Layer 3 features on the aggregate interface instead of on the member ports. If you configure any Layer 3 feature mistakenly on a member port, remove the Layer 3 feature configuration from the member port and then run the `shutdown` and `undo shutdown` commands on the aggregate interface.

- Removing an aggregate interface also removes the corresponding aggregation group. At the same time, all member ports leave the aggregation group.

- You cannot change the working mode (bridging or routing) of the member ports in an aggregation group.

- You can assign only ports on the same type of cards to an aggregation group when the router works in hybrid mode. For example, after assigning ports on an SPE card to an aggregation group, you cannot assign ports on an SPC card to the aggregation group.

### Configuring a static aggregation group

**NOTE:**

To guarantee a successful static aggregation, make sure that the ports at both ends of each link are in the same aggregation state.
Configuring a Layer 2 static aggregation group

To configure 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</td>
</tr>
<tr>
<td>3.</td>
<td>Exit to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Assign an Ethernet interface to the aggregation group.</td>
<td>- Enter Layer 2 Ethernet interface view: interface interface-type interface-number - Assign the Ethernet interface to the aggregation group: port link-aggregation group number</td>
</tr>
<tr>
<td>5.</td>
<td>Assign the port an aggregation priority.</td>
<td>link-aggregation port-priority port-priority</td>
</tr>
</tbody>
</table>

Configuring a Layer 3 static aggregation group

To configure 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</td>
</tr>
<tr>
<td>2.</td>
<td>Create a Layer 3 aggregate interface and enter Layer 3 aggregate interface view.</td>
<td>interface route-aggregation 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 Ethernet interface to the aggregation group.</td>
<td>- Enter Layer 3 Ethernet interface view: interface interface-type interface-number - Assign the Ethernet interface to the aggregation group: port link-aggregation group number</td>
</tr>
</tbody>
</table>
5. Assign the port an aggregation priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>link-aggregation port-priority port-priority</td>
<td>Optional. By default, the aggregation priority of a port is 32768. Changing the aggregation priority of a port may affect the aggregation state of the ports in the static aggregation group.</td>
</tr>
</tbody>
</table>

Configuring a dynamic aggregation group

NOTE:

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

Configuring a Layer 2 dynamic aggregation group

To configure 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>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>lacp system-priority system-priority</td>
<td>Optional. By default, the system LACP priority is 32768. Changing the system LACP priority may affect the aggregation state of the ports in a dynamic aggregation group.</td>
</tr>
<tr>
<td>3.</td>
<td>interface bridge-aggregation interface-number</td>
<td>When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 static aggregation group numbered the same.</td>
</tr>
<tr>
<td>4.</td>
<td>link-aggregation mode dynamic</td>
<td>By default, an aggregation group works in static aggregation mode.</td>
</tr>
<tr>
<td>5.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type interface-number • Assign the Ethernet interface to the aggregation group: port link-aggregation group number</td>
<td>Repeat this step to assign more Layer 2 Ethernet interfaces to the aggregation group.</td>
</tr>
</tbody>
</table>
### Configuring a Layer 3 dynamic aggregation group

To configure a Layer 3 dynamic aggregation group:

<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>lACP system-priority system-priority</td>
<td>By default, the system LACP priority is 32768. Changing the system LACP priority may affect the aggregation state of the ports in the dynamic aggregation group.</td>
</tr>
<tr>
<td>3.</td>
<td>interface route-aggregation</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.</td>
<td>link-aggregation mode dynamic</td>
<td>By default, an aggregation group works in static aggregation mode.</td>
</tr>
<tr>
<td>5.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td>• Enter Layer 3 Ethernet interface view: interface interface-type interface-number&lt;br&gt;• Assign the Ethernet interface to the aggregation group: port link-aggregation group number</td>
<td>Repeat this step to assign more Layer 3 Ethernet interfaces to the aggregation group.</td>
</tr>
</tbody>
</table>
7. Assign the port an aggregation priority.
   
   **Command:**
   - `link-aggregation port-priority`  
   - `port-priority`

   **Remarks:**
   Optional.  
   By default, the aggregation priority of a port is 32768.  
   Changing the aggregation priority of a port may affect the aggregation state of ports in the dynamic aggregation group.

8. Set the LACP timeout interval on the port to the short timeout interval (1 second).
   
   **Command:**
   - `lacp period short`

   **Remarks:**
   Optional.  
   By default, the LACP timeout interval on a port is the long timeout interval (30 seconds).

---

### Configuring an aggregate interface

You can perform the following configurations on an aggregate interface:

- Configuring the description of an aggregate interface or subinterface
- Configuring the MTU of a Layer 3 aggregate interface or subinterface
- Enabling link state traps for an aggregate interface
- Setting the minimum number of Selected ports for an aggregation group
- Shutting down an aggregate interface
- Restoring the default settings for an aggregate interface

### Configuring the description of an aggregate interface or subinterface

You can configure the description of an aggregate interface for administration purposes such as describing the purpose of the interface.

To configure the description of an aggregate interface or subinterface:

<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.   | - 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 }`  
   | Use either command. |
Configuring the MTU of a Layer 3 aggregate interface or subinterface

The maximum transmission unit (MTU) of an interface affects IP packets fragmentation and reassembly on the interface.

To change the MTU of a Layer 3 aggregate 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>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 aggregate interface or subinterface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the MTU of the Layer 3 aggregate interface or subinterface.</td>
<td>Optional. The default setting is 1500 bytes.</td>
</tr>
</tbody>
</table>

Enabling link state traps for an aggregate interface

You can configure an aggregate interface to generate linkUp trap messages when its link goes up and linkDown trap messages when its link goes down. For more information, see Network Management and Monitoring Configuration Guide.

To enable link state traps on 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>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the trap function globally.</td>
<td>Optional. By default, link state trapping is enabled globally and on all interfaces.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter aggregate interface view.</td>
<td>Use either command.</td>
</tr>
</tbody>
</table>

- Enter Layer 2 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
Setting the minimum number of Selected ports for an aggregation group

The bandwidth of an aggregate link increases along with the number of selected member ports. To avoid congestion caused by insufficient Selected ports on an aggregate link, you can set the minimum number of Selected ports required for bringing up the specific aggregate interface.

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

- All member ports change to the Unselected state and the link of the aggregate interface goes down, when the number of member ports eligible for being selected is smaller than the minimum threshold.
- When the minimum threshold is reached, the eligible member ports change to the Selected state, and the link of the aggregate interface goes up.

To set the minimum number 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></td>
<td>- Enter Layer 2 aggregate interface view:</td>
<td>interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>2.</td>
<td>Enter aggregate interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter Layer 3 aggregate interface view:</td>
<td>interface route-aggregation interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the minimum number of Selected ports for the aggregation group.</td>
<td>link-aggregation selected-port minimum number</td>
</tr>
</tbody>
</table>

⚠️ CAUTION:

- If you set this minimum threshold for a static aggregation group, you must also make the same setting for its peer aggregation group to guarantee correct aggregation.
- Configuring the minimum number of Selected ports required to bring up an aggregation group may cause all the member ports in the current aggregation group to become unselected.
Shutting down an aggregate interface

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

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

To shut down 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 aggregate interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view:</td>
<td>interface bridge-aggregation</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 3 aggregate interface or subinterface view:</td>
<td>interface route-aggregation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Shut down the aggregate interface or subinterface.</td>
<td>shutdown</td>
</tr>
<tr>
<td></td>
<td>By default, aggregate interfaces or subinterfaces are up.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

Shutting down an aggregate subinterface does not affect any aggregation group, because an aggregate subinterface does not have an associated aggregation group.

Restoring the default settings for an aggregate interface

To restore the default settings for 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 aggregate interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 aggregate interface view:</td>
<td>interface bridge-aggregation</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 3 aggregate interface or subinterface view:</td>
<td>interface route-aggregation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-number.subnumber }</td>
</tr>
<tr>
<td>3.</td>
<td>Restore the default settings for the aggregate interface or subinterface.</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Configuring load sharing criteria for link aggregation groups

You can determine how traffic is load-shared in a link aggregation group by configuring load sharing criteria. The criteria can be MPLS labels, service port numbers, IP addresses, MAC addresses, or receiving ports carried in packets, or any combination.

To configure the global link-aggregation load sharing criteria:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2. Configure the global link-aggregation load sharing criteria.</td>
<td>link-aggregation load-sharing mode { destination-ip</td>
</tr>
</tbody>
</table>

**NOTE:**

Only SPC cards support the configuration of link-aggregation load sharing criteria. Even though you can configure the `link-aggregation load-sharing mode` command on SPE cards, the command does not take effect.

Displaying and maintaining Ethernet link aggregation

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information for an aggregate interface or multiple aggregate interfaces.</td>
<td>display interface [ bridge-aggregation</td>
<td>route-aggregation ] [ brief</td>
</tr>
<tr>
<td>Display the local system ID.</td>
<td>display lacp system-id [</td>
<td></td>
</tr>
<tr>
<td>Display the global link-aggregation load sharing criteria.</td>
<td>display link-aggregation load-sharing mode [ interface [ bridge-aggregation</td>
<td>route-aggregation ] interface-number ] [</td>
</tr>
<tr>
<td>Display detailed link aggregation information for link aggregation member ports.</td>
<td>display link-aggregation member-port [ interface-list ] [</td>
<td></td>
</tr>
<tr>
<td>Display summary information about all aggregation groups.</td>
<td>display link-aggregation summary [</td>
<td></td>
</tr>
</tbody>
</table>
### Task | Command | Remarks
--- | --- | ---
Display detailed information about a specific or all aggregation groups. | `display link-aggregation verbose [{ bridge-aggregation | route-aggregation } [ interface-number ] | { begin | exclude | include } regular-expression ]` | Available in any view

Clear LACP statistics for a specific or all link aggregation member ports. | `reset lacp statistics [ interface interface-list ]` | Available in user view

Clear statistics for a specific or all aggregate interfaces. | `reset counters interface [{ bridge-aggregation | route-aggregation } [ interface-number ] ]` | Available in user view

---

**Ethernet link aggregation configuration examples**

**NOTE:**

In an aggregation group, only ports that have the same port attributes and class-two configurations (see “Configuration classes”) as the reference port (see “Reference port”) can operate as Selected ports. Make sure that all member ports have the same port attributes and class-two configurations as the reference port. The other settings only need to be configured on the aggregate interface, not on the member ports.

---

**Layer 2 static aggregation configuration example**

**Network requirements**

As shown in Figure 26:

- Configure a Layer 2 static aggregation group 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, and VLAN 20 at one end to communicate with VLAN 20 at the other end.

- Enable traffic to be load-shared across aggregation group member ports based on the source and destination MAC addresses.

**Figure 26 Network diagram**

1. Configure Device A:
# Create VLAN 10, and assign port GigabitEthernet 4/1/4 to VLAN 10.
[DeviceA] system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 4/1/4
[DeviceA-vlan10] quit

# Create VLAN 20, and assign port GigabitEthernet 4/1/5 to VLAN 20.
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 4/1/5
[DeviceA-vlan20] quit

# Create Layer 2 aggregate interface Bridge-Aggregation 1.
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit

# Assign ports GigabitEthernet 4/1/1 through GigabitEthernet 4/1/3 to link aggregation group 1.
[DeviceA] interface gigabitethernet 4/1/1
[DeviceA-GigabitEthernet4/1/1] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/1] quit
[DeviceA] interface gigabitethernet 4/1/2
[DeviceA-GigabitEthernet4/1/2] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/2] quit
[DeviceA] interface gigabitethernet 4/1/3
[DeviceA-GigabitEthernet4/1/3] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/3] 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
Please wait... Done.
Configuring GigabitEthernet4/1/1... Done.
Configuring GigabitEthernet4/1/2... Done.
Configuring GigabitEthernet4/1/3... Done.
[DeviceA-Bridge-Aggregation1] quit

# Configure Device A to use the source and destination MAC addresses of packets as the global link-aggregation load sharing criteria.
[DeviceA] link-aggregation load-sharing mode source-mac destination-mac

2. Configure Device B:
Configure Device B using the same instructions that you used to configure Device A.

3. Verify the configurations:
# Display summary information about all aggregation groups on Device A.
[DeviceA] display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001
The output shows that link aggregation group 1 is a load shared Layer 2 static aggregation group and it contains three Selected ports.

# Display the global link-aggregation load sharing criteria on Device A.

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

```
Link-Aggregation Load-Sharing Mode:
  destination-mac address, source-mac address
```

The output shows that all link aggregation groups created on the device perform load sharing based on source and destination MAC addresses.

**Layer 2 dynamic aggregation configuration example**

**Network requirements**

As shown in Figure 27:

- Configure a Layer 2 dynamic aggregation group 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, and VLAN 20 at one end to communicate with VLAN 20 at the other end.
- Enable traffic to be load-shared across aggregation group member ports based on source and destination MAC addresses.

**Figure 27 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure Device A:

```
# Create VLAN 10, and assign the port GigabitEthernet 4/1/4 to VLAN 10.
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 4/1/4
[DeviceA-vlan10] quit
```
# Create VLAN 20, and assign the port GigabitEthernet 4/1/5 to VLAN 20.
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 4/1/5
[DeviceA-vlan20] quit

# Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the link aggregation mode as dynamic.
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic

# Assign ports GigabitEthernet 4/1/1 through GigabitEthernet 4/1/3 to link aggregation group 1 one at a time.
[DeviceA] interface gigabitethernet 4/1/1
[DeviceA-GigabitEthernet4/1/1] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/1] quit

[DeviceA] interface gigabitethernet 4/1/2
[DeviceA-GigabitEthernet4/1/2] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/2] quit

[DeviceA] interface gigabitethernet 4/1/3
[DeviceA-GigabitEthernet4/1/3] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/3] 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

Please wait... Done.
Configuring GigabitEthernet4/1/1... Done.
Configuring GigabitEthernet4/1/2... Done.
Configuring GigabitEthernet4/1/3... Done.
[DeviceA-Bridge-Aggregation1] quit

# Configure the device to use the source and destination MAC addresses of packets as the global link-aggregation load sharing criteria.
[DeviceA] link-aggregation load-sharing mode source-mac destination-mac

2. Configure Device B:
Configure Device B using the same instructions that you used to configure Device A.

3. Verify the configurations:

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

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

<table>
<thead>
<tr>
<th>AGG</th>
<th>AGG</th>
<th>Partner ID</th>
<th>Select</th>
<th>Unselect</th>
<th>Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Mode</td>
<td>Ports</td>
<td>Ports</td>
<td>Type</td>
<td></td>
</tr>
</tbody>
</table>

---------------------------------------------
Layer 3 static aggregation configuration example

**Network requirements**

As shown in Figure 28:

- Configure a Layer 3 static aggregation group on Device A and Device B respectively and configure IP addresses and subnet masks for the corresponding Layer 3 aggregate interfaces.
- Enable traffic to be load-shared across aggregation group member ports based on source and destination IP addresses.

**Figure 28 Network diagram**

![Network Diagram](image)

**Configuration procedure**

1. Configure Device A:
   
   # CreateLayer 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 GigabitEthernet 4/interfaces GigabitEthernet 4/1/1 through GigabitEthernet 4/1/3 to aggregation group 1.
   [DeviceA] interface gigabitethernet 4/1/1
   [DeviceA-GigabitEthernet4/1/1] port link-aggregation group 1
   [DeviceA-GigabitEthernet4/1/1] quit
   [DeviceA] interface gigabitethernet 4/1/2
   [DeviceA-GigabitEthernet4/1/2] port link-aggregation group 1
   [DeviceA-GigabitEthernet4/1/2] quit
   [DeviceA] interface gigabitethernet 4/1/3
   [DeviceA-GigabitEthernet4/1/3] port link-aggregation group 1
   [DeviceA-GigabitEthernet4/1/3] quit
   # Configure the global link-aggregation load sharing criteria as the source and destination IP addresses of packets.
   ```
2. Configure Device B:
Configure Device B using the same instructions that you used to configure Device A.

3. Verify the configurations:
# Display summary information about all aggregation groups on Device A.
[DeviceA] display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

<table>
<thead>
<tr>
<th>AGG</th>
<th>AGG</th>
<th>Partner ID</th>
<th>Select</th>
<th>Unselect</th>
<th>Share</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAGG1</td>
<td>S</td>
<td>none</td>
<td>3</td>
<td>0</td>
<td>Shar</td>
</tr>
</tbody>
</table>

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

# Display the global link-aggregation load sharing criteria on Device A.
[DeviceA] display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:

destination-ip address, source-ip address

The output shows that the global link-aggregation load sharing criteria are the source and destination IP addresses of packets.

Layer 3 dynamic aggregation configuration example

Network requirements
As shown in Figure 29:
- Configure a Layer 3 dynamic aggregation group on Device A and Device B respectively and configure IP addresses and subnet masks for the corresponding Layer 3 aggregate interfaces.
- Enable traffic to be load-shared across aggregation group member ports based on source and destination IP addresses.

Figure 29 Network diagram

Configuration procedure
1. Configure Device A:
# Create Layer 3 aggregate interface Route-Aggregation 1, configure the link aggregation mode as dynamic, and configure an IP address and subnet mask for the aggregate interface.
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit

# Assign Layer 3 Ethernet interfaces GigabitEthernet 4/1/1 through GigabitEthernet 4/1/3 to aggregation group 1.
[DeviceA] interface gigabitethernet 4/1/1
[DeviceA-GigabitEthernet4/1/1] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/1] quit
[DeviceA] interface gigabitethernet 4/1/2
[DeviceA-GigabitEthernet4/1/2] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/2] quit
[DeviceA] interface gigabitethernet 4/1/3
[DeviceA-GigabitEthernet4/1/3] port link-aggregation group 1
[DeviceA-GigabitEthernet4/1/3] quit

# Configure Device A to use the source and destination IP addresses of packets as the global link-aggregation load sharing criteria.
[DeviceA] link-aggregation load-sharing mode source-ip destination-ip

2. Configure Device B:
Configure Device B using the same instructions that you used to as you configure Device A.

3. Verify the configurations

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

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e2ff-0001

<table>
<thead>
<tr>
<th>AGG</th>
<th>AGG</th>
<th>Partner ID</th>
<th>Select</th>
<th>Unselect</th>
<th>Share</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0x8000, 000f-e2ff-0002</td>
<td>3</td>
<td>0</td>
<td>Shar</td>
</tr>
</tbody>
</table>

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

# Display the global link-aggregation load sharing criteria on Device A.
[DeviceA] display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
destination-ip address, source-ip address

The output shows that the global link-aggregation load sharing criteria are the source and destination IP addresses of packets.
Configuring port isolation

Introduction to port isolation

Assigning ports to different VLANs is a typical way to isolate Layer 2 traffic for data privacy and security, but this way is VLAN resource demanding. To save VLAN resources, you can use the port isolation feature, which can isolate ports without using VLANs and allows for great flexibility and security.

For the isolated ports to communicate with a port outside isolation groups at Layer 2, you must configure one uplink port for an isolation group.

The number of ports in an isolation group is not limited.

NOTE:

- You cannot configure a link aggregation member port as the uplink port of an isolation group neither can you assign the uplink port of an isolation group to a link aggregation group. If a port is configured as a link aggregation member port and the uplink port of an isolation group at the same time, which is allowed with some old version software, the link aggregation group configuration will take effect while the port group configuration is removed for compatibility sake after you upgrade the configuration file. For more information about link aggregation, see the chapter “Configuring Ethernet link aggregation.”

- Isolated ports only support MAC address learning, QoS actions accounting, filter deny, and car cir committed-information-rate red discard, and traffic mirroring in the incoming direction of the actions.

- H3C does not recommend that you configure Layer 2 protocols (such as GVRP) or Layer 3 protocols (such as multicast and routing) on isolated ports. Doing so can cause forwarding anomaly or protocol flapping.

Layer 2 traffic cannot be forwarded between ports in different VLANs. However, the Layer 2 traffic from an isolated port can pass through the uplink port in the same isolation group unidirectionally even if they belong to different VLANs.

Figure 30 Communication between ports in the same VLAN in port isolation
Configuring an isolation group

Assigning ports to an isolation group

To assign ports 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-number</td>
</tr>
</tbody>
</table>

3. Enter interface view or port group view.

- Enter Ethernet interface view:
  ```
  interface interface-type interface-number
  ```
- Enter port group view:
  ```
  port-group manual port-group-name
  ```
- Enter Layer 2 aggregate interface view:
  ```
  interface bridge-aggregation interface-number
  ```

4. Assign ports to an isolation group as isolated ports.

- Use one of the commands.
- To assign Ethernet ports to the isolation group one by one, perform the command in Ethernet interface view.
- To bulk assign Ethernet ports to the isolation group, perform the command in port group view.
- The configuration in Layer 2 aggregate interface view applies to the Layer 2 aggregate interface and its aggregation member ports. If the router 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 router skips the port and continues to assign other aggregation member ports to the isolation group.

```
port-isolate enable group group-number
```

No ports are assigned to any isolation group by default.

Specifying the uplink port for an isolation group

To specify the uplink port for 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>
</tbody>
</table>
2. Enter interface view.

- Enter Ethernet interface view:
  ```
  interface interface-type
  interface-number
  ```

- Enter Layer 2 aggregate interface view:
  ```
  interface bridge-aggregation
  interface-number
  ```

Use either command.

- The configuration in Ethernet interface view applies only to the port.
- In Layer 2 aggregate interface view, only the Layer 2 aggregate interface is configured as the uplink port of the specified isolation group, and you can still assign its member ports as isolated ports. However, these ports will be placed in Unselected state and cannot receive or forward data packets.

3. Configure the port as the uplink port of an isolation group.

- **port-isolate uplink-port group**
  ```
  group-number
  ```

An isolation group has no uplink port by default.

**NOTE:**

- An isolation group can have only one uplink port. The uplink port you configured for an isolation group can overwrite the previous one, if any.
- If you configure a common port in an isolation group as the common port of another isolation group, the port leaves the previous group and joins the new one.
- You cannot configure an isolated port in an isolation group as the uplink port in any isolation group.
- You cannot configure the uplink port of an isolation group as an isolated or uplink port in any other isolation group.
- You cannot configure a link aggregation member port as the uplink port of an isolation group neither can you assign the uplink port of an isolation group to a link aggregation group.

### Displaying and maintaining isolation groups

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the isolation group information.</td>
<td><code>display port-isolate group [group-number]</code> [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>

### Port isolation configuration example

**Networking requirement**

As shown in Figure 31:

- Device is connected to an external networks through GigabitEthernet 3/1/4.
- GigabitEthernet 3/1/1, GigabitEthernet 3/1/2, GigabitEthernet 3/1/3 and GigabitEthernet 3/1/4 belong to the same VLAN.
Configure that Host A, Host B, and Host C cannot exchange Layer 2 traffic with each other, but can access the external network.

**Figure 31 Networking diagram**

![Networking Diagram]

**Configuration procedure**

# Create isolation group 2.

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

# Add GigabitEthernet 3/1/1, GigabitEthernet 3/1/2, and GigabitEthernet 3/1/3 to isolation group 2 as isolated ports.

```bash
[Device] interface GigabitEthernet 3/1/1
[Device-GigabitEthernet3/1/1] port-isolate enable group 2
[Device-GigabitEthernet3/1/1] quit
[Device] interface GigabitEthernet 3/1/2
[Device-GigabitEthernet3/1/2] port-isolate enable group 2
[Device-GigabitEthernet3/1/2] quit
[Device] interface GigabitEthernet 3/1/3
[Device-GigabitEthernet3/1/3] port-isolate enable group 2
[Device-GigabitEthernet3/1/3] quit
```

# Configure GigabitEthernet 3/1/4 as the uplink port of isolation group 2.

```bash
[Device] interface GigabitEthernet 3/1/4
[Device-GigabitEthernet3/1/4] port-isolate uplink-port group 2
[Device-GigabitEthernet3/1/4] return
```

# Display information about isolation group 2.

```bash
<Device> display port-isolate group 2
Port-isolate group information:
Uplink port support: YES
Group ID: 2
Uplink port: GigabitEthernet3/1/4
Group members:
    GigabitEthernet3/1/1    GigabitEthernet3/1/2     GigabitEthernet3/1/3
```
NOTE:
In this documentation, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L, and SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

Introduction to QinQ

802.1Q in 802.1Q (QinQ) is a flexible, easy-to-implement Layer 2 VPN technology based on IEEE 802.1Q. It enables the edge router on the service provider network to encapsulate an outer VLAN tag in Ethernet frames from customer networks (private networks), so that the Ethernet frames will travel across the service provider network (public network) with double VLAN tags. QinQ enables a service provider to use a single provider network VLAN (SVLAN) to serve customers who have multiple customer network VLANs (CVLANs).

Background and benefits

The IEEE 802.1Q VLAN tag uses 12 bits for VLAN IDs. A network device supports a maximum of 4094 VLANs, which is far from enough for isolating users in actual networks, especially in metropolitan area networks (MANs).

By tagging tagged frames, QinQ expands the available VLAN space from 4094 to $4094 \times 4094$. QinQ delivers the following benefits:

- Releases the stress on the SVLAN resource.
- Enables customers to plan their CVLANs without conflicting with SVLANs.
- Provides an easy-to-implement Layer 2 VPN solution for small-sized MANs or intranets.
- Allows the customers to keep their current network configurations when the service provider upgrades the service provider network, thus making the customer networks more independent.

How QinQ works

The devices in the public network forward a frame only according to its outer VLAN tag and learn its source MAC address into the MAC address table of the outer VLAN. The inner VLAN tag of the frame is transmitted as payload.

NOTE:
- All QinQ-related configurations are made on the service provider network only.
- Because QinQ is based on the IEEE 802.1Q protocol, all network devices through which QinQ packets may pass must support the IEEE 802.1Q protocol.
As shown in Figure 32, customer network A has CVLANs 1 through 10, while customer network B has CVLANs 1 through 20. The SVLAN allocated by the service provider for customer network A is SVLAN 3, and for customer network B is SVLAN 4. When a tagged Ethernet frame of customer network A enters the service provider network, it is tagged with outer VLAN 3; when a tagged Ethernet frame of customer network B enters the service provider network, it is tagged with outer VLAN 4. In this way, there is no overlap of VLAN IDs among customers, and traffic from different customers can be separated.

**QinQ frame structure**

A QinQ frame is transmitted double-tagged over the service provider network. As shown in Figure 33, the inner VLAN tag is the CVLAN tag, and the outer one is the SVLAN tag that the service provider has allocated to the customer.

**Figure 33 Single-tagged Ethernet frame header and double-tagged Ethernet frame header**

<table>
<thead>
<tr>
<th>Single-tagged frame structure</th>
<th>Double-tagged frame structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bytes DA</td>
<td>6 bytes SA</td>
</tr>
<tr>
<td>6 bytes DA</td>
<td>6 bytes SA</td>
</tr>
</tbody>
</table>

**NOTE:**

The default maximum transmission unit (MTU) of an interface is 1500 bytes. The size of an outer VLAN tag is 4 bytes. H3C recommends you to increase the MTU of each interface on the service provider network to at least 1504 bytes. For more information about interface MTU configuration, see *Interface Configuration Guide.*
Implementations of QinQ

The router supports basic QinQ only.

Basic QinQ enables a port to tag any incoming frames with its port VLAN (PVID) tag, regardless of whether they have been tagged or not. If an incoming frame has been tagged, it becomes a double-tagged frame. If not, it becomes a frame tagged with the port’s PVID tag.

Modifying the TPID value in a VLAN tag

A VLAN tag uses the tag protocol identifier (TPID) field to identify the protocol type of the tag. The default TPID value is 0x8100.

Figure 34 VLAN Tag structure of an Ethernet frame

The router determines whether a received frame carries a service provider VLAN tag or a customer VLAN tag by checking the corresponding TPID value. Upon receiving a frame, the router compares the configured TPID value with the value of the TPID field in the frame. If the two match, the frame carries the corresponding VLAN tag. For example, if a frame carries VLAN tags with the TPID value of 0x9200 whereas the configured TPID value of the service provider VLAN tag is 0x9100, the router considers that the frame does not carry the service provider VLAN tag.

In addition, the systems of different vendors may set the TPID of the outer VLAN tag of QinQ frames to different values. For compatibility with these systems, you can modify the TPID value so that the QinQ frames, when sent to the public network, carry the TPID value identical to the value of a particular vendor to allow interoperability with network devices of that vendor.

The TPID in an Ethernet frame has the same position with the protocol type field in a frame without a VLAN tag. To avoid problems in packet forwarding and handling in the network, you cannot set the TPID value to any of the values in Table 14.

Table 14 Reserved protocol type 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>
</tbody>
</table>
Protocols and standards

IEEE 802.1Q: IEEE standard for local and metropolitan area networks: Virtual Bridged Local Area Networks

QinQ configuration task list

Complete the follows tasks to configure QinQ:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring basic QinQ</td>
<td>Required</td>
</tr>
<tr>
<td>Setting the TPID value in VLAN tags</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**NOTE:**
- QinQ requires configurations only on the service provider network.
- Do not configure QinQ on a reflector port. For more information about reflector ports, see Network Management and Monitoring Configuration Guide.

Configuring basic QinQ

To enable basic QinQ:

<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 view or port group view.</td>
<td><code>interface interface-type</code> <code>interface-number</code>&lt;br&gt;<code>port-group manual port-group-name</code>&lt;br&gt;Use either command.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable QinQ on the port(s).</td>
<td><code>qinq enable</code></td>
</tr>
</tbody>
</table>

**NOTE:**
Configure basic QinQ on the user-to-network interfaces (UNIs) on service provider network devices that connect the user networks.
Setting the TPID value in VLAN tags

To set the TPID value in outer VLAN 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 interface view or port group view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface interface-type interface-number</td>
<td>Use either command.</td>
</tr>
<tr>
<td></td>
<td>- Enter port group view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-group manual port-group-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Set the TPID value in outer VLAN tags.</td>
<td>qinq ethernet-type hex-value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE:
To change a non-default TPID value to another non-default TPID value, you must first restore the default TPID value (0x8100) on an SPE card, but you can directly change the TPID value on an SPC card.

Basic QinQ configuration example

Network requirements

As shown in Figure 35:
- The two branches of Company A, Site 1 and Site 2, are connected through the service provider network and use CVLANs 10 through 70. The two branches of Company B, Site 3 and Site 4, are connected through the service provider network and use CVLANs 30 through 90.
- PE 1 and PE 2 are edge devices on the service provider network and are connected through third-party devices with a TPID value of 0x8200.

Configure the edge and third-party devices to enable communication between the branches of Company A through SVLAN 100, and communication between the branches of Company B through SVLAN 200.
NOTE:
Make sure that the devices in the service provider network have been configured to allow QinQ packets to pass through.

1. Configure PE 1:
   # Configure GigabitEthernet 3/1/1 as a trunk port and assign it to VLAN 100 and VLANs 10 through 70.
   <PE1> system-view
   [PE1] interface GigabitEthernet 3/1/1
   [PE1-GigabitEthernet3/1/1] port link-type trunk
   [PE1-GigabitEthernet3/1/1] port trunk permit vlan 100 10 to 70
   # Configure VLAN 100 as the PVID for the port.
   [PE1-GigabitEthernet3/1/1] port trunk pvid vlan 100
   # Enable basic QinQ on the port.
   [PE1-GigabitEthernet3/1/1] qinq enable
   [PE1-GigabitEthernet3/1/1] quit
   # Configure GigabitEthernet 3/1/2 as a trunk port and assign it to VLAN 100 and VLAN 200.
   [PE1] interface GigabitEthernet 3/1/2
   [PE1-GigabitEthernet3/1/2] port link-type trunk
   [PE1-GigabitEthernet3/1/2] port trunk permit vlan 100 200 200
   # Set the TPID value in the outer VLAN tag to 0x8200 on the port.
   [PE1-GigabitEthernet3/1/2] qinq ethernet-type 8200
   [PE1-GigabitEthernet3/1/2] quit
   # Configure GigabitEthernet 3/1/3 as a trunk port and assign it to VLAN 200 and VLANs 30 through 90.
2. Configure PE 2:

# Configure GigabitEthernet 3/1/1 as a trunk port and assign it to VLAN 200 and VLANs 30 through 90.

<PE2> system-view
[PE2] interface GigabitEthernet 3/1/1
[PE2-GigabitEthernet3/1/1] port link-type trunk
[PE2-GigabitEthernet3/1/1] port trunk permit vlan 200 30 to 90
# Configure VLAN 200 as the PVID for the port.
[PE2-GigabitEthernet3/1/1] port trunk pvid vlan 200
# Enable basic QinQ on the port.
[PE2-GigabitEthernet3/1/1] qinq enable
[PE2-GigabitEthernet3/1/1] quit

# Configure GigabitEthernet 3/1/2 as a trunk port and assign it to VLAN 100 and VLAN 200.

[PE2] interface GigabitEthernet 3/1/2
[PE2-GigabitEthernet3/1/2] port link-type trunk
[PE2-GigabitEthernet3/1/2] port trunk permit vlan 100 200
# Set the TPID value in the outer VLAN tag to 0x8200 on the port.
[PE2-GigabitEthernet3/1/2] qinq ethernet-type 8200
[PE2-GigabitEthernet3/1/2] quit

# Configure GigabitEthernet 3/1/3 as a trunk port and assign it to VLAN 100 and VLANs 10 through 70.

[PE2] interface GigabitEthernet 3/1/3
[PE2-GigabitEthernet3/1/3] port link-type trunk
[PE2-GigabitEthernet3/1/3] port trunk permit vlan 100 10 to 70
# Configure VLAN 100 as the PVID for the port.
[PE2-GigabitEthernet3/1/3] port trunk pvid vlan 100
# Enable basic QinQ on the port.
[PE2-GigabitEthernet3/1/3] qinq enable
[PE2-GigabitEthernet3/1/3] quit

3. Configure third-party devices:

On the third-party devices between PE 1 and PE 2, configure the port connecting to PE 1 and that connecting to PE 2 to allow tagged frames of VLAN 100 and VLAN 200 to pass through.
Configuring BPDU tunneling

Introduction to BPDU tunneling

As a Layer 2 tunneling technology, BPDU tunneling enables Layer 2 protocol packets from geographically dispersed customer networks to be transparently transmitted over specific tunnels across a service provider network.

Background

Dedicated lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a user network is broken down into parts located at different sides of the service provider network. As shown in Figure 36, User A has two devices (CE 1 and CE 2) and both devices belong to VLAN 100. User A’s network is divided into network 1 and network 2, which are connected by the service provider network. When a Layer 2 protocol (for example, STP) runs on both network 1 and network 2, the Layer 2 protocol packets must be transmitted over the service provider network to implement Layer 2 protocol calculation (for example, spanning tree calculation). When receiving a Layer 2 protocol packet, the PEs cannot determine whether the packet is from the user network or the service provider network, and must deliver the packet to the CPU for processing. In this case, the Layer 2 protocol calculation in User A’s network is mixed with that in the service provider network, and the user network cannot implement independent Layer 2 protocol calculation.

Figure 36 BPDU tunneling application scenario

With BPDU tunneling, Layer 2 protocol packets from customer networks can be transparently transmitted over the service provider network in the following workflow:

1. After receiving a Layer 2 protocol packet from CE 1, PE 1 in the service provider network encapsulates the packet, replaces its destination MAC address with a specific multicast MAC address, and then forwards the packet in the service provider network;

2. The encapsulated Layer 2 protocol packet (called bridge protocol data unit, BPDU) is forwarded to PE 2 at the other end of the service provider network, which de-encapsulates the packet, restores the original destination MAC address of the packet, and then sends the packet to CE 2.

NOTE:

BPDU tunneling supports the transparent transmission of the Spanning Tree Protocol (STP) packets.
BPDU Tunneling implementation

NOTE:
- The term STP in this document is in a broad sense. It includes STP, RSTP, and MSTP.
- STP calculates the topology of a network by transmitting BPDUs among bridges in the network. For details, see the chapter “Configuring the spanning tree.”

To avoid loops in your network, you can enable STP on your routers. When the topology changes at one side of the customer network, the routers at this side of the customer network send BPDUs to routers on the other side of the customer network, thus ensuring consistent spanning tree calculation in the entire customer network. However, because BPDUs are Layer 2 multicast frames, all STP-enabled routers, both in the customer network and in the service provider network, can receive and process these BPDUs. In this case, neither the service provider network nor the customer network can correctly calculate its independent spanning tree.

To allow each network to calculate an independent spanning tree with STP, BPDU tunnelling was introduced.

BPDU tunnelling delivers the following benefits:
- BPDUs can be transparently transmitted. BPDUs of the same customer network can be broadcast in a specific VLAN across the service provider network, so that the geographically dispersed networks of the same customer can implement consistent spanning tree calculation across the service provider network.
- BPDUs of different customer networks can be confined within different VLANs for transmission on the service provider network. Thus, each customer network can perform independent spanning tree calculation.

![Figure 37 BPDU tunneling implementation](image)

As shown in Figure 37, the upper part is the service provider network (ISP network), and the lower part represents two different parts of a customer network: User A network 1 and User A network 2. Enabling the BPDU tunnelling function on the edge routers (PE 1 and PE 2) in the service provider network allows BPDUs of the customer network to be transparently transmitted in the service provider network, thus ensuring consistent spanning tree calculation of User A network, without affecting the spanning tree calculation of the service provider network.

Assume a BPDU is sent from User A network 1 to User A network 2:
1. At the ingress of the service provider network, PE 1 changes the destination MAC address of the BPDU from 0x0180-C200-0000 to a special multicast MAC address, 0x010F-E200-0003 (the
default multicast MAC address) for example. In the service provider network, the modified BPDU is forwarded as a data packet in the VLAN assigned to User A.

2. At the egress of the service provider network, PE 2 recognizes the BPDU with the destination MAC address 0x010F-E200-0003, restores its original destination MAC address 0x0180-C200-0000, and then sends the BPDU to CE 2.

NOTE:
Make sure, through configuration, that the VLAN tags carried in BPDUs are neither changed nor removed during the transparent transmission in the service provider network; otherwise, the routers in the service provider network will fail to transparently transmit the customer network BPDUs correctly.

Configuring BPDU tunneling

Configuration prerequisites

- Before configuring BPDU tunneling for STP, enable STP in the customer network first.
- Before enabling BPDU tunneling for STP on a port, disable STP on the port first.
- Assign the port on which you want to enable BPDU tunneling on the PE router and the connected port on the CE router to the same VLAN.
- Configure ports connecting routers in the service provider network as trunk ports allowing packets of any VLAN to pass through.

Enabling BPDU tunneling for a protocol

This section describes how to enable BPDU tunneling for STP. You can enable BPDU tunneling for GVRP in a similar way.

To enable BPDU tunneling for STP:

<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 or port group view.</td>
<td>Use any command. Settings made in Layer 2 Ethernet/aggregate interface view take effect only on the current port. Settings made in port group view take effect on all ports in the port group.</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 port group view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-group manual port-group-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Disable STP.</td>
<td>stp disable</td>
</tr>
<tr>
<td>4.</td>
<td>Enable BPDU tunneling for STP.</td>
<td>bpdu-tunnel dot1q stp</td>
</tr>
</tbody>
</table>
Configuring destination multicast MAC address for BPDUs

By default, the destination multicast MAC address for BPDUs is 0x010F-E200-0003. You can change it to 0x0100-0CCD-CDD0, 0x0100-0CCD-CDD1 or 0x0100-0CCD-CDD2 through the following configuration.

To configure the destination multicast MAC address for 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>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the destination multicast MAC address for BPDUs.</td>
<td>bpdu-tunnel tunnel-dmac mac-address</td>
</tr>
</tbody>
</table>

NOTE:

For BPDUs to be recognized, the destination multicast MAC addresses configured for BPDUs must be the same on the edge routers on the service provider network.

BPDU tunneling configuration example

Network requirements

As shown in Figure 38:

- CE 1 and CE 2 are edges routers on the geographically dispersed network of User A; PE 1 and PE 2 are edge routers on the service provider network.
- All ports that connect service provider and customer routers are access ports and belong to VLAN 2; all ports that connect service provider routers are trunk ports and allow packets of any VLAN to pass through.
- MSTP is enabled on User A network.

Configure BPDU tunneling, so that CE 1 and CE 2 implement consistent spanning tree calculation across the service provider network and the destination multicast MAC address in BPDUs is 0x0100-0CCD-CDD0.

Figure 38 Network diagram

Configuration procedure

1. Configure PE 1:
# Configure the destination multicast MAC address for BPDUs as 0x0100-0CCD-CDD0.
<Sysname> system-view
[Sysname] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0

# Create VLAN 2 and assign GigabitEthernet 3/1/1 to VLAN 2.
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface GigabitEthernet 3/1/1
[Sysname-GigabitEthernet3/1/1] port access vlan 2

# Disable STP on GigabitEthernet 3/1/1, and then enable BPDU tunneling for STP on it.
[Sysname-GigabitEthernet3/1/1] stp disable
[Sysname-GigabitEthernet3/1/1] bpdu-tunnel dot1q stp

2. Configure PE 2:

# Configure the destination multicast MAC address for BPDUs as 0x0100-0CCD-CDD0.
<Sysname> system-view
[Sysname] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0

# Create VLAN 2 and assign GigabitEthernet 3/1/2 to VLAN 2.
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 3/1/2
[Sysname-GigabitEthernet3/1/2] port access vlan 2

# Disable STP on GigabitEthernet 3/1/2, and then enable BPDU tunneling for STP on it.
[Sysname-GigabitEthernet3/1/2] stp disable
[Sysname-GigabitEthernet3/1/2] bpdu-tunnel dot1q stp
Configuring GVRP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby network devices in a bridged LAN, such as end stations and switches, can register and deregister attribute values. The GARP VLAN Registration Protocol (GVRP) is a GARP application that registers and deregisters VLAN attributes. GVRP uses the operating mechanism of GARP to maintain and propagate dynamic VLAN registration information for the GVRP devices on the network.

Introduction to GVRP

GARP

GARP provides a mechanism that allows participants in a GARP application to distribute, propagate, and register with other participants in a LAN the attributes specific to the GARP application, such as the VLAN or multicast address attributes.

How GARP works

Each port that participates in a GARP application (GVRP for example) is a GARP participant. Through the GARP mechanism, the attribute information of GARP participants is rapidly propagated across the entire LAN. As shown in Figure 39, a GARP participant registers and deregisters its attribute information with other GARP participants by sending and withdrawing declarations, and registers and deregisters the attribute information of other participants according to the declarations and withdrawals it receives.

Figure 39 How GARP works

For example, GVRP registers and deregisters VLAN attributes as follows:

- When a port receives a declaration for a VLAN attribute, it registers the VLAN attribute carried in the declaration, and joins the VLAN.
- When a port receives a withdrawal for a VLAN attribute, it deregisters the VLAN attribute carried in the withdrawal, and leaves the VLAN.

GARP messages

A GARP participant exchanges information with other GARP participants by sending GARP messages, including Join, Leave, and LeaveAll. These messages work together to ensure the registration and de-registration of attribute information. As a GARP application, GVRP also uses GARP messages for information exchange.
1. **Join messages**

   A GARP participant sends Join messages when it wants to register its attributes (including manually configured attributes) on other participants, and when it receives Join messages from other participants. There are two types of Join messages: JoinEmpty and JoinIn.
   - A GARP participant sends a JoinEmpty message to declare an attribute not registered on it.
   - A GARP participant sends a JoinIn message to declare an attribute registered on it.

2. **Leave messages**

   A GARP participant sends Leave messages to have its attributes deregistered on other participants. It also sends Leave messages when it deregisters attributes after receiving Leave messages from other GARP participants, and when attributes are manually deregistered on it. There are two types of Leave messages: LeaveEmpty and LeaveIn.
   - A GARP participant sends a LeaveEmpty message to deregister an attribute not registered on it.
   - A GARP participant sends a LeaveIn message to deregister an attribute registered on it.

3. **LeaveAll messages**

   Each GARP participant starts a LeaveAll timer upon startup. Upon the expiration of the LeaveAll timer, a GARP participant sends LeaveAll messages to deregister all attributes so that all attributes can be re-registered on the other GARP participants. When a GARP participant receives LeaveAll messages from other GARP participants, it also sends LeaveAll messages and reset the LeaveAll timer.

---

**GARP timers**

---

**NOTE:**

- The settings of GARP timers apply to all GARP applications, such as GVRP, on a LAN.
- On a GARP-enabled network, each port of a network device maintains its own Hold, Join, and Leave timers, but only one LeaveAll timer is maintained on each device globally.
- The value ranges for the Hold, Join, Leave, and LeaveAll timers are dependent on one another. For more information, see Table 16.

---

GARP defines the following timers to control the sending of GARP messages:

1. **Hold timer**

   The Hold timer sets the delay that a GARP participant waits before sending a Join or Leave message.

   When an attribute value changes or a Join or Leave message arrives, the GARP participant does not send the message immediately. Rather, it assembles Join and Leave messages in the least number of GARP PDUs, and sends them out when the Hold timer expires. This timer reduces the number of GARP PDUs and saves bandwidth.

2. **Join timer**

   A GARP participant may declare an attribute twice to ensure reliable transmission. The Join timer sets the interval between the two declarations.

   A GARP participant starts a Join timer when it declares an attribute value or receives a JoinIn message for the attribute value. If the GARP participant does not receive any declaration for the attribute value when the Join timer expires, it re-declares the attribute value.
NOTE:
Because all attributes of a GARP participant share the same Join timer, you must set the Join timer long enough so that all attributes can be sent out in one declaration.

3. Leave timer
A GARP participant starts a Leave timer when it receives a Leave message for an attribute value. If the GARP participant has not received a Join message for the attribute value before the timer expires, it deregisters the attribute value.

4. LeaveAll timer
Upon startup, a GARP participant starts a LeaveAll timer. When this timer expires, the participant sends a LeaveAll message so that other participants can re-register all its attribute information. Then, the LeaveAll timer restarts to begin a new cycle. The LeaveAll timer and all other GARP timers also restart when the GARP participant receives a LeaveAll message.

NOTE:
- Do not set the LeaveAll timer too short, because a LeaveAll message deregisters all attributes in the entire network. The LeaveAll timer must be greater than Leave timers on all ports. H3C recommends that you set a LeaveAll timer no less than the default value (1000 centiseconds).
- On a GARP-enabled network, a device may send LeaveAll messages at the interval set by its LeaveAll timer or the LeaveAll timer of another device on the network, whichever is smaller. This is because each time a device on the network receives a LeaveAll message, it resets its LeaveAll timer.

GARP PDU format

Figure 40 GARP PDU format

Ethernet frame

As shown in Figure 40, GARP PDUs use the IEEE 802.3 Ethernet frame format.

Table 15 The GARP PDU fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol ID</td>
<td>Protocol identifier for GARP</td>
<td>0x0001</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Message</td>
<td>One or multiple messages, each containing an attribute type and an attribute list</td>
<td>N/A</td>
</tr>
<tr>
<td>End mark</td>
<td>Indicates the end of a GARP PDU</td>
<td>0x00</td>
</tr>
<tr>
<td>Attribute type</td>
<td>Defined by the GARP application</td>
<td>0x01 for GVRP, indicating the VLAN ID attribute</td>
</tr>
<tr>
<td>Attribute list</td>
<td>Contains one or multiple attributes</td>
<td>N/A</td>
</tr>
<tr>
<td>Attribute length</td>
<td>Length of an attribute, inclusive of the attribute length field</td>
<td>2 to 255 (in bytes)</td>
</tr>
<tr>
<td>Attribute event</td>
<td>Event described by the attribute</td>
<td>• 0x00 — LeaveAll event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x01 — JoinEmpty event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x02 — JoinIn event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x03 — LeaveEmpty event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x04 — LeaveIn event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0x05 — Empty event</td>
</tr>
<tr>
<td>Attribute value</td>
<td>Attribute value</td>
<td>VLAN ID for GVRP</td>
</tr>
</tbody>
</table>

The destination MAC addresses of GARP messages are multicast MAC addresses, and vary with GARP applications. For example, the destination MAC address of GVRP is 01-80-C2-00-00-21. A network device distributes GARP messages to different GARP applications according to the destination MAC addresses carried in GARP messages.

**GVRP**

**GVRP overview**

As a GARP application, GVRP enables a network device to propagate local VLAN registration information to other participant devices, and to dynamically update the VLAN registration information from other devices to its local database, including active VLAN members and through which port they can be reached. This makes sure that all GVRP participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

**GVRP registration modes**

VLANs manually created are called static VLANs, and VLANs created by GVRP are called dynamic VLANs. GVRP provides three registration modes on a port, including Normal, Fixed, and Forbidden. In different registration modes, a port handles static and dynamic VLANs differently:

- **Normal**—Allows dynamic creation, registration, and deregistration of VLANs on the trunk port.
- **Fixed**—Allows manual creation and registration of VLANs, prevents VLAN deregistration, and registers all known VLANs on other ports on the trunk port.
• **Forbidden**—Deregisters all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port.

**Protocols and standards**
- IEEE 802.1Q, Virtual Bridged Local Area Networks

**GVRP configuration task list**

Complete these tasks to configure GVRP:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring GVRP functions</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring GARP timers</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**NOTE:**
- GVRP configuration made in Ethernet interface view or Layer-2 aggregate interface view takes effect on the current interface only. GVRP configuration made in port group view takes effect on all the member ports in the group.
- GVRP configuration made on a member port in an aggregation group takes effect only after the port is removed from the aggregation group.

**Configuring GVRP functions**

Before enabling GVRP on a port, you must enable GVRP globally. In addition, GVRP can be configured only on trunk ports, and you must assign the involved trunk ports to all dynamic VLANs.

To configure GVRP functions on a trunk 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>Enable GVRP globally.</td>
<td>gvrp</td>
</tr>
</tbody>
</table>
| 3.   | Enter Ethernet interface view, Layer 2 aggregate interface view, or port-group view. | • Enter Ethernet interface view or Layer 2 aggregate interface view: interface interface-type interface-number  
      • Enter port-group view: port-group manual port-group-name | Use either command. |
<p>| 4.   | Configure the link type of the ports as trunk. | port link-type trunk                         | The default setting is access. |
| 5.   | Assign the trunk ports to all VLANs.   | port trunk permit vlan all                   | By default, a trunk port is assigned to VLAN 1 only. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>gvrp</td>
<td>By default, GVRP is disabled on a port.</td>
</tr>
<tr>
<td>7.</td>
<td>gvrp registration { fixed</td>
<td>forbidden</td>
</tr>
</tbody>
</table>

**NOTE:**
- For more information about the `port link-type trunk` and `port trunk permit vlan all` commands, see *Layer 2—LAN Switching Command Reference*.
- GVRP is mutually exclusive with service loopback.
- GVRP can work with STP, RSTP, or MSTP CIST. When GVRP runs on the CIST, blocked ports on the CIST cannot receive/send GVRP packets. For more information about STP, RSTP, and MSTP CIST, see the chapter “Configuring the spanning tree.”
- Do not enable both GVRP and remote port mirroring. Otherwise, GVRP may register the remote probe VLAN to unexpected ports, resulting in undesired duplicates to be received by the monitor port. For more information about port mirroring, see *Network Management and Monitoring Configuration Guide*.
- Enabling GVRP on a Layer 2 aggregate interface enables both the aggregate interface and all selected member ports in the corresponding link aggregation group to participate in dynamic VLAN registration and deregistration.

### Configuring GARP timers

Among the four GARP timers, the LeaveAll timer is configured in system view and takes effect on all ports, while the other three are configured on a port basis.

To configure GARP 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>garp timer leaveall timer-value</td>
<td>Optional. The default setting is 1000 centiseconds.</td>
</tr>
<tr>
<td>3.</td>
<td>interface interface-type interface-number</td>
<td>Use either command. Depending on the view you accessed, the subsequent configuration takes effect on a port or all ports in a port-group.</td>
</tr>
<tr>
<td>4.</td>
<td>garp timer hold timer-value</td>
<td>Optional. The default setting is 10 centiseconds.</td>
</tr>
</tbody>
</table>
5. Configure the Join timer.
   `garp timer join timer-value`
   Optional. The default setting is 20 centiseconds.

6. Configure the Leave timer.
   `garp timer leave timer-value`
   Optional. The default setting is 60 centiseconds.

As shown in Table 16, the value ranges for GARP timers are dependent on one another:

- If you want to set a value beyond the value range for a timer, you may change the value range by tuning the value of another related timer.
- If you want to restore the default settings of the timers, restore the Hold timer first, and then the Join, Leave, and LeaveAll timers.

**Table 16 Dependencies of GARP timers**

<table>
<thead>
<tr>
<th>Timer</th>
<th>Lower limit</th>
<th>Upper limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold</td>
<td>10 centiseconds</td>
<td>No greater than half of the Join timer setting</td>
</tr>
<tr>
<td>Join</td>
<td>No less than twice the Hold timer setting</td>
<td>Less than half of the Leave timer setting</td>
</tr>
<tr>
<td>Leave</td>
<td>Greater than twice the Join timer setting</td>
<td>Less than the LeaveAll timer setting</td>
</tr>
<tr>
<td>LeaveAll</td>
<td>Greater than the Leave timer setting</td>
<td>32765 centiseconds</td>
</tr>
</tbody>
</table>

**NOTE:**

To keep the dynamic VLANs learned through GVRP stable, do not set the LeaveAll timer smaller than its default value (1000 centiseconds).

## Displaying and maintaining GVRP

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display GARP statistics on ports.</td>
<td>`display garp statistics [ interface interface-list ] [</td>
<td></td>
</tr>
<tr>
<td>Display GARP timers on ports.</td>
<td>`display garp timer [ interface interface-list ] [</td>
<td></td>
</tr>
<tr>
<td>Display the local VLAN information</td>
<td>`display gvrp local-vlan interface interface-type interface-number [</td>
<td></td>
</tr>
<tr>
<td>maintained by GVRP on ports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display the current GVRP state in the</td>
<td>`display gvrp state interface interface-number vlan vlan-id [</td>
<td></td>
</tr>
<tr>
<td>specified VLANs on ports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display GVRP statistics on ports.</td>
<td>`display gvrp statistics [ interface interface-list ] [</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Display the global GVRP state.</td>
<td>display gvrp status [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the information about dynamic VLAN operations on ports.</td>
<td>display gvrp vlan-operation interface interface-type interface-number [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Clear the GARP statistics on ports.</td>
<td>reset garp statistics [ interface interface-list ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

**GVRP configuration examples**

**GVRP normal registration mode configuration example**

**Network requirements**

As shown in Figure 41, Device A and Device B are connected through their GigabitEthernet 4/1/1 ports. Enable GVRP and configure the normal registration mode on ports to enable the registration of dynamic and static VLAN information between the two routers.

**Figure 41 Network diagram**

![Network diagram](image)

**Figure 41 Network diagram**

| Device A | Device B |

**Configuration procedure**

1. Configure Device A:

   # Enable GVRP globally.
   <DeviceA> system-view
   [DeviceA] gvrp

   # Configure port GigabitEthernet 4/1/1 as a trunk port, and assign it to all VLANs.
   [DeviceA] interface GigabitEthernet 4/1/1
   [DeviceA-GigabitEthernet4/1/1] port link-type trunk
   [DeviceA-GigabitEthernet4/1/1] port trunk permit vlan all

   # Enable GVRP on trunk port GigabitEthernet 4/1/1.
   [DeviceA-GigabitEthernet4/1/1] gvrp
   [DeviceA-GigabitEthernet4/1/1] quit

   # Create VLAN 2 (a static VLAN).
   [DeviceA] vlan 2
   [DeviceA-vlan2] quit

2. Configure Device B:

   # Enable GVRP globally.
   <DeviceB> system-view
   [DeviceB] gvrp

   # Configure port GigabitEthernet 4/1/1 as a trunk port, and assign it to all VLANs.
[DeviceB] interface GigabitEthernet 4/1/1
[DeviceB-GigabitEthernet4/1/1] port link-type trunk
[DeviceB-GigabitEthernet4/1/1] port trunk permit vlan all

# Enable GVRP on trunk port GigabitEthernet 4/1/1.
[DeviceB-GigabitEthernet4/1/1] gvrp
[DeviceB-GigabitEthernet4/1/1] quit

# Create VLAN 3 (a static VLAN).
[DeviceB] vlan 3
[DeviceB-vlan3] quit

3. Verify the configuration:

Use the `display gvrp local-vlan` command to display the local VLAN information maintained by GVRP on ports. For example:

# Display the local VLAN information maintained by GVRP on port GigabitEthernet 4/1/1 of Device A.
[DeviceA] display gvrp local-vlan interface GigabitEthernet 4/1/1
Following VLANs exist in GVRP local database:
1(default),2-3

According to the output above, information about VLAN 1, static VLAN information of VLAN 2 on the local router, and dynamic VLAN information of VLAN 3 on Device B are all registered through GVRP.

# Display the local VLAN information maintained by GVRP on port GigabitEthernet 4/1/1 of Device B.
[DeviceB] display gvrp local-vlan interface GigabitEthernet 4/1/1
Following VLANs exist in GVRP local database:
1(default),2-3

The output shows that information about VLAN 1, static VLAN information of VLAN 3 on the local router, and dynamic VLAN information of VLAN 2 on Device A are all registered through GVRP.

GVRP fixed registration mode configuration example

Network requirements

As shown in Figure 42, Device A and Device B are connected through their GigabitEthernet 4/1/1 ports.

Enable GVRP and configure the fixed registration mode on ports to enable the registration of static VLAN information between the two routers.

Figure 42 Network diagram

![Network Diagram](image)

Configuration procedure

1. Configure Device A:

   # Enable GVRP globally.

   <DeviceA> system-view
   [DeviceA] gvrp
# Configure port GigabitEthernet 4/1/1 as a trunk port, and assign it to all VLANs.

```
[DeviceA] interface GigabitEthernet 4/1/1
[DeviceA-GigabitEthernet4/1/1] port link-type trunk
[DeviceA-GigabitEthernet4/1/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet 4/1/1 and set the GVRP registration mode to fixed on the port.

```
[DeviceA-GigabitEthernet4/1/1] gvrp
[DeviceA-GigabitEthernet4/1/1] gvrp registration fixed
[DeviceA-GigabitEthernet4/1/1] quit
```

# Create VLAN 2 (a static VLAN).

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

2. Configure Device B:

# Enable GVRP globally.

```
<DeviceB> system-view
[DeviceB] gvrp
```

# Configure port GigabitEthernet 4/1/1 as a trunk port, and assign it to all VLANs.

```
[DeviceB] interface GigabitEthernet 4/1/1
[DeviceB-GigabitEthernet4/1/1] port link-type trunk
[DeviceB-GigabitEthernet4/1/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet 4/1/1, and set the GVRP registration mode to fixed on the port.

```
[DeviceB-GigabitEthernet4/1/1] gvrp
[DeviceB-GigabitEthernet4/1/1] gvrp registration fixed
[DeviceB-GigabitEthernet4/1/1] quit
```

# Create VLAN 3 (a static VLAN).

```
[DeviceB] vlan 3
[DeviceB-vlan3] quit
```

3. Verify the configuration:

Use the `display gvrp local-vlan` command to display the local VLAN information maintained by GVRP on ports. For example:

# Display the local VLAN information maintained by GVRP on port GigabitEthernet 4/1/1 of Device A.

```
[DeviceA] display gvrp local-vlan interface GigabitEthernet 4/1/1
Following VLANs exist in GVRP local database:
  1(default), 2
```

According to the output above, information about VLAN 1 and static VLAN information of VLAN 2 on the local router are registered through GVRP, but dynamic VLAN information of VLAN 3 on Device B is not.

# Display the local VLAN information maintained by GVRP on port GigabitEthernet 4/1/1 of Device B.

```
[DeviceB] display gvrp local-vlan interface GigabitEthernet 4/1/1
Following VLANs exist in GVRP local database:
  1(default), 3
```
According to the output above, information about VLAN 1 and static VLAN information of VLAN 3 on the local router are registered through GVRP, but dynamic VLAN information of VLAN 2 on Device A is not.

**GVRP forbidden registration mode configuration example**

**Network requirements**

As shown in Figure 43, Device A and Device B are connected through their GigabitEthernet 4/1/1 ports.

Enable GVRP and configure the forbidden registration mode on ports to prevent the registration of all VLANs but VLAN 1 between the two routers.

![Figure 43 Network diagram](image)

**Configuration procedure**

1. **Configure Device A:**
   
   ```
   # Enable GVRP globally.
   <DeviceA> system-view
   [DeviceA] gvrp
   # Configure port GigabitEthernet 4/1/1 as a trunk port, and assign it to all VLANs.
   [DeviceA] interface GigabitEthernet 4/1/1
   [DeviceA-GigabitEthernet4/1/1] port link-type trunk
   [DeviceA-GigabitEthernet4/1/1] port trunk permit vlan all
   # Enable GVRP on GigabitEthernet 4/1/1, and set the GVRP registration mode to forbidden on the port.
   [DeviceA-GigabitEthernet4/1/1] gvrp
   [DeviceA-GigabitEthernet4/1/1] gvrp registration forbidden
   [DeviceA-GigabitEthernet4/1/1] quit
   # Create VLAN 2 (a static VLAN).
   [DeviceA] vlan 2
   [DeviceA-vlan2] quit
   ```

2. **Configure Device B:**

   ```
   # Enable GVRP globally.
   <DeviceB> system-view
   [DeviceB] gvrp
   # Configure port GigabitEthernet 4/1/1 as a trunk port, and assign it to all VLANs.
   [DeviceB] interface GigabitEthernet 4/1/1
   [DeviceB-GigabitEthernet4/1/1] port link-type trunk
   [DeviceB-GigabitEthernet4/1/1] port trunk permit vlan all
   # Enable GVRP on GigabitEthernet 4/1/1, and set the GVRP registration mode to forbidden on the port.
   [DeviceB-GigabitEthernet4/1/1] gvrp
   [DeviceB-GigabitEthernet4/1/1] gvrp registration forbidden
   ```
3. Verify the configuration:

Use the `display gvrp local-vlan` command to display the local VLAN information maintained by GVRP on ports. For example:

```bash
# Display the local VLAN information maintained by GVRP on port GigabitEthernet 4/1/1 of Device A.
[DeviceA] display gvrp local-vlan interface GigabitEthernet 4/1/1
Following VLANs exist in GVRP local database:
  1 (default)
According to the output above, information about VLAN 1 is registered through GVRP, but static VLAN information of VLAN 2 on the local router and dynamic VLAN information of VLAN 3 on Device B are not.
```

```bash
# Display the local VLAN information maintained by GVRP on port GigabitEthernet 4/1/1 of Device B.
[DeviceB] display gvrp local-vlan interface GigabitEthernet 4/1/1
Following VLANs exist in GVRP local database:
  1 (default)
According to the output above, information about VLAN 1 is registered through GVRP, but static VLAN information of VLAN 3 on the local router and dynamic VLAN information of VLAN 2 on Device A are not.
```
Configuring VLAN termination

NOTE:
- In this documentation, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L, and SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.
- Only the SPE cards support VLAN termination.

Overview

Introduction to VLAN termination

VLAN termination refers to the following packet processing procedure:
- A port receives a VLAN-tagged packet, removes its VLAN tag(s) and then forwards it via Layer 3 or processes it in other ways. Whether the packet is tagged before being sent out depends on the port configuration.
- Before sending a packet, the port adds related VLAN information to it.

VLAN termination types

Based on the number of tags a VLAN-tagged packet carries, the VLAN-tagged packets falls into the following types:
- Dot1q packet (also known as an 802.1q packet), which carries a single VLAN tag
- QinQ packet, which carries double VLAN tags

Accordingly, VLAN termination falls into the following types:
- **Dot1q termination**—Terminates Dot1q packets and removes a Dot1q packet’s single VLAN tag.
- **QinQ termination**—Terminates QinQ packets and removes a QinQ packet’s inner and outer VLAN tags.

NOTE:
- The router only supports QinQ termination.
- A Layer 3 Ethernet interface cannot process VLAN-tagged packets, but you can create subinterfaces for it to process VLAN-tagged packets.
- A Layer 3 Ethernet subinterface receives and sends only VLAN-tagged packets.

Application scenarios

VLAN termination is mainly used for the following purposes:
- Inter-VLAN communication
- LAN-WAN communication
Inter-VLAN communication

VLAN technology is widely used to isolate Layer 2 packets. It divides a LAN into multiple virtual LANs (VLANs) with each being a broadcast domain. Hosts within a VLAN can communicate with each other directly, whereas hosts in different VLANs are isolated at Layer 2. To allow different VLANs to communicate, Layer 3 routing must be used. You can configure the following methods to implement VLAN communication:

- Configuring VLAN interfaces on routers, as shown in Figure 44.
- Configuring Layer 3 Ethernet subinterfaces on routers, as shown in Figure 45.

As shown in Figure 44 and Figure 45, Host A belongs to VLAN 2, and Host B belongs to VLAN 3. After you specify Host A’s gateway IP address as 1.1.1.1/24 and Host B’s gateway IP address as 1.1.2.1/24, Host A and Host B can communicate at Layer 3 through VLAN interfaces or Layer 3 Ethernet subinterfaces.

LAN-WAN communication

Most packets sent out LANs carry VLAN tags, but some WAN protocols such as ATM, Frame Relay, and PPP cannot recognize VLAN tagged packets. Therefore, before sending VLAN-tagged packets to a
WAN, the sending port must record and remove the VLAN information of the packets. VLAN interfaces or Layer 3 Ethernet subinterfaces can be used for LAN-WAN communication.

As shown in Figure 46, the VLANs of the customer network are called customer VLANs (CVLANs), and the VLANs of the service provider network are called service provider VLANs (SVLANs). When a packet carrying a CVLAN tag enters the service provider network, it is tagged with a SVLAN tag, and forwarded based on the SVLAN tag. When the packet is to be forwarded to an external WAN, the gateway (Device) must perform VLAN termination for the packet and remove the two layers of VLAN tags from the packet before sending the packet to the WAN.

**Figure 46 VLAN termination enables LAN-WAN communication**

1. Add a CVLAN tag
2. Enable QinQ, and add a SVLAN tag
3. Create a Layer 3 Ethernet subinterface or VLAN interface to perform QinQ termination

VLAN termination configuration task list

Complete the following tasks to configure VLAN termination:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring TPID for VLAN-tagged packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling a QinQ termination-enabled interface/subinterface to transmit broadcast and multicast packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring QinQ termination</td>
<td>Required</td>
</tr>
</tbody>
</table>

Configuring TPID for VLAN-tagged packets

IEEE 802.1Q inserts a four-byte VLAN tag field between the DA&SA field and the type field to carry VLAN-related information in an Ethernet frame header. Figure 47 shows the subfields in the VLAN tag field in Ethernet II encapsulation. Other Ethernet encapsulation formats include 802.2 LLC, 802.2 SNAP, and 802.3 raw. Figure 48 compares the structure of a Dot1q packet and that of a QinQ packet.

**Figure 47 Subfields in the VLAN Tag field**

<table>
<thead>
<tr>
<th>VLAN Tag</th>
<th>DA&amp;SA</th>
<th>TPID</th>
<th>Priority</th>
<th>CFI</th>
<th>VLAN ID</th>
<th>Type</th>
</tr>
</thead>
</table>

**Figure 48**

No figure reference mentioned.
**Figure 48 Compare the structure of a Dot1q packet and that of a QinQ packet**

The VLAN tag field contains the following subfields: Tag Protocol Identifier (TPID), Priority, Canonical Format Indicator (CFI), and VLAN ID. Among these four subfields, TPID indicates whether an Ethernet packet carries a VLAN tag, or whether the packet is a VLAN-tagged packet. The TPID subfield contains 16 bits and usually takes the value of 0x8100. However, each vendor can define their own TPID value.

To enable the interfaces to recognize VLAN-tagged packets whose TPID is not 0x8100 and communicate with other vendors’ devices, the router provides the TPID configuration function. After TPID is configured,

- When receiving a packet, the device processes the packet according to Table 17.

**Table 17 TPID-based processing for a received packet**

<table>
<thead>
<tr>
<th>TPID in outer VLAN tag</th>
<th>TPID in inner VLAN tag</th>
<th>Process the packet as…</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8100 or the user-defined value</td>
<td>0x8100</td>
<td>A QinQ packet</td>
</tr>
<tr>
<td>Not 0x8100 or the user-defined value</td>
<td>N/A</td>
<td>An untagged Ethernet packet</td>
</tr>
</tbody>
</table>

- When sending out a packet, the router processes the packet according to Table 18.

**Table 18 TPID-based processing for a packet to be sent**

<table>
<thead>
<tr>
<th>Whether a TPID value is defined by the user</th>
<th>Set the TPID in the outer VLAN tag to…</th>
<th>Set the TPID in the inner VLAN tag to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>User-defined value</td>
<td>• 0x8100 if the packet has an inner VLAN tag</td>
</tr>
<tr>
<td>No</td>
<td>0x8100</td>
<td>• not set the TPID value if the packet has no inner VLAN tag</td>
</tr>
</tbody>
</table>

**NOTE:**

- If the current interface is up, upon the configuration of the TPID value, the interface will be shut down and then brought up to have the configuration take effect.

- Even if you have used the `dot1q ethernet-type` command to define a TPID value other than 0x8100, the device always processes packets with TPID value 0x8100 as VLAN-tagged packets. However, when the device sends out a packet, it sets the packet’s TPID to the user-defined value.

- The TPID values set on the local and peer devices must be consistent. Otherwise, packets may fail to be transmitted properly.
**Configuring TPID on a Layer 3 Ethernet/aggregate subinterface**

To configure VLAN termination on a Layer 3 Ethernet subinterface or Layer 3 aggregate subinterface, follow these steps to configure the TPID value in the outer VLAN tag of packets received and sent by the 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>
</tbody>
</table>
| 2.   | Enter interface view. | • Enter Layer 3 Ethernet interface view: `interface interface-type interface-number`  
• Enter Layer 3 aggregate interface view: `interface route-aggregation interface-number` | Use either command. Configurations made in Layer 3 Ethernet interface view take effect on all subinterfaces. Configurations made in Layer 3 aggregate interface view take effect on all the Layer 3 aggregate subinterfaces of the interface. |
| 3.   | Set the TPID value in the outer VLAN tag of packets received and sent by the interface. | `dot1q ethernet-type hex-value` | Optional. By default, the TPID value in the outer VLAN tag is 0x8100. If the interface receives and sends QinQ packets, the TPID value in the inner VLAN tag of packets is always 0x8100, and is not configurable. |

If not specified, the TPID value in the outer VLAN tag of packets takes the default value 0x8100.

**Configuring TPID on a Layer 2 Ethernet or aggregate interface**

To configure VLAN termination on a VLAN interface, set the TPID value in the outer VLAN tag of packets received and sent by Layer 2 physical interfaces in the corresponding VLAN. If not specified, the TPID value in the outer VLAN tag of packets takes the default value 0x8100.

To set the TPID value for VLAN-tagged packets on a Layer 2 Ethernet or 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>
</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` | Use either command. Configurations made in Layer 2 aggregate interface view take effect on all the member interfaces in the aggregation group. |
3. Set the TPID value in the outer VLAN tag of packets received and sent by the interface.

   **Command**: `qinq ethernet-type [service-tag] hex-value`

   **Remarks**: Optional.
   By default, the TPID value in the outer VLAN tag is 0x8100.
   If the interface receives and sends QinQ packets, the TPID value in the inner VLAN tag of packets is always 0x8100, and is not configurable.

---

**NOTE:**
For more information about the `qinq ethernet-type` command, see Layer 2—LAN Switching Command Reference.

### Enabling a QinQ termination-enabled interface/subinterface to transmit broadcast and multicast packets

By default, an ambiguous QinQ termination-enabled subinterface or VLAN interface drops broadcast and multicast packets it receives, instead of transmitting them.

You can enable an ambiguous QinQ termination-enabled Layer 3 Ethernet/aggregate subinterface or VLAN interface to transmit broadcast and multicast packets.

To enable an ambiguous QinQ termination-enabled Layer 3 Ethernet/aggregate subinterface or VLAN interface to transmit broadcast and multicast 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><code>system-view</code></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 3 Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface interface-type interface-number.subnumber</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 3 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface route-aggregation interface-number.subnumber</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter VLAN interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface vlan-interface interface-number</code></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Enable the QinQ termination-enabled subinterface or VLAN interface to transmit broadcast and multicast packets.</td>
<td><code>vlan-termination broadcast enable</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a QinQ termination-enabled Layer 3 Ethernet/aggregate subinterface or VLAN interface does not transmit broadcast and multicast packets.</td>
</tr>
</tbody>
</table>
Configuring QinQ termination

Based on the range of VLAN IDs in the VLAN-tagged packets that can be terminated by a subinterface, QinQ termination falls into the following two categories:

- **Unambiguous QinQ termination**—Terminates QinQ packets with the specified inner VLAN ID and outer VLAN ID. Any other QinQ packet is not allowed to pass through this subinterface. When a packet is sent out the subinterface, the packet is tagged with two VLAN tags as specified.

- **Ambiguous QinQ termination**—Terminates VLAN-tagged packets with the specified outer VLAN ID and the inner VLAN IDs in the specified range. These QinQ packets may have different inner VLAN IDs. VLAN-tagged packets whose inner VLAN IDs are not in the range are not allowed to pass through this subinterface. When a packet is sent out the subinterface, the packet is tagged with the specified outer VLAN ID and an inner VLAN ID: for an IPv4/MPLS packet, the inner VLAN ID is obtained by searching the ARP entries; for a PPPoE packet, the inner VLAN ID is obtained by searching the PPPoE session entries; for a DHCP relay packet, the inner VLAN ID is obtained by searching the DHCP session entries.

Configuring unambiguous QinQ termination

To configure unambiguous QinQ termination on a Layer 3 Ethernet subinterface, Layer 3 aggregate subinterface, or VLAN 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>Use one of the commands.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable QinQ termination on the subinterface or VLAN interface, and configure the subinterface or VLAN interface to terminate the QinQ packets with the specified inner VLAN ID.</td>
<td>second-dot1q vlan-id</td>
</tr>
</tbody>
</table>

**NOTE:**

After you enable QinQ termination on a VLAN interface, Layer 2 Ethernet interfaces in the corresponding VLAN process only QinQ packets destined for the VLAN interface, and drop Dot1q and non-VLAN-tagged packets.
Configuring ambiguous QinQ termination

To configure ambiguous QinQ termination on a Layer 3 Ethernet/aggregate subinterface or VLAN 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></td>
<td>• Enter Layer 3 Ethernet interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface interface-type interface-number.subnumber</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 3 aggregate interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface route-aggregation interface-number.subnumber</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter VLAN interface view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface vlan-interface interface-number</td>
<td></td>
</tr>
</tbody>
</table>

2. Enter interface view. Use one of the commands.

3. Enable QinQ termination on the subinterface or VLAN interface, and configure the subinterface or VLAN interface to terminate the QinQ packets with the specified inner VLAN ID.

    second-dot1q { any | vlan-id-list }

    The outer VLAN ID of the QinQ packets that can be terminated by the current subinterface or VLAN interface is the interface number, and is not configurable.

**NOTE:**

After you enable QinQ termination on a VLAN interface, Layer 2 Ethernet interfaces in the corresponding VLAN process only QinQ packets destined for the VLAN interface, and drop Dot1q and non-VLAN-tagged packets.

VLAN termination configuration examples

**NOTE:**

Only the SPE cards support VLAN termination.

Unambiguous QinQ termination configuration example

**Network requirements**

As shown in Figure 49, Host A connects to Switch A and belongs to VLAN 11. Host B connects to Switch C, which supports only single VLAN-tagged packets. With QinQ enabled, Switch B adds an outer VLAN tag with VLAN ID 100 to Dot1q packets carrying inner VLAN ID 11 before forwarding them. Host A needs to be able to communicate with Host B.
Configuration procedure

1. Configure Host A and Host B:
   - Configure Host A’s IP address as 1.1.1.1/24, and gateway IP address as 1.1.1.11/24.
   - Configure Host B’s IP address as 1.1.2.1/24, and gateway IP address as 1.1.2.11/24.

2. Configure Switch A:
   ```
   <SwitchA> system-view
   [SwitchA] vlan 11
   [SwitchA-vlan11] port ethernet 1/2
   [SwitchA-vlan11] quit
   [SwitchA] interface ethernet 1/1
   [SwitchA-Ethernet1/1] port link-type trunk
   [SwitchA-Ethernet1/1] port trunk permit vlan 11
   Please wait... Done.
   ```

3. Configure Switch B:
   ```
   <SwitchB> system-view
   [SwitchB] interface ethernet 1/2
   [SwitchB-Ethernet1/2] port link-type trunk
   [SwitchB-Ethernet1/2] port trunk permit vlan 11 100
   Please wait... Done.
   [SwitchB-Ethernet1/2] qinq enable
   [SwitchB-Ethernet1/2] qinq vid 100
   [SwitchB-Ethernet1/2-vid-100] raw-vlan-id inbound 11
   [SwitchB-Ethernet1/2-vid-100] quit
   [SwitchB-Ethernet1/2] quit
   [SwitchB] interface ethernet 1/1
   [SwitchB-Ethernet1/1] port link-type trunk
   [SwitchB-Ethernet1/1] port trunk permit vlan 100
   ```

4. Configure the router:
# Create Ethernet subinterface GigabitEthernet 2/1/7.100 and enter subinterface view. Assign an IP address to the Ethernet subinterface, enable QinQ termination on it, and specify the inner VLAN ID of the QinQ packets that can be terminated by it.

```
<Router> system-view
[Router] interface GigabitEthernet2/1/7.100
[Router-GigabitEthernet2/1/7.100] ip address 1.1.1.11 255.255.255.0
[Router-GigabitEthernet2/1/7.100] second-dot1q 11
[Router-GigabitEthernet2/1/7.100] quit
[Router] interface GigabitEthernet 2/1/6
[Router-GigabitEthernet2/1/6] ip address 1.1.2.11 255.255.255.0
```

5. Configure Switch C:
Use Switch C’s factory configuration.

## Ambiguous QinQ termination configuration example

### Network requirements

As shown in Figure 50, Host A, Host B and Host C are connected to Switch A and they belong to VLAN 11, VLAN 12 and VLAN 13 respectively. The server group is connected to Switch C. QinQ is enabled on Switch B. Host A, Host B, and Host C need to communicate with the server group.

![Network diagram](image)

**Figure 50 Network diagram**

### Configuration procedure

1. Configure Host A, Host B, and Host C:
   - Configure Host A’s IP address as 1.1.1.1/24, and gateway IP address as 1.1.1.11/24.
   - Configure Host B’s IP address as 1.1.1.2/24, and gateway IP address as 1.1.1.11/24.
   - Configure Host C’s IP address as 1.1.1.3/24, and gateway IP address as 1.1.1.11/24.

2. Configure Switch A:
   ```
   <SwitchA> system-view
   ```
[SwitchA] vlan 11
[SwitchA-vlan11] port ethernet 1/1
[SwitchA-vlan11] quit
[SwitchA] vlan 12
[SwitchA-vlan12] port ethernet 1/2
[SwitchA-vlan12] quit
[SwitchA] vlan 13
[SwitchA-vlan13] port ethernet 1/3
[SwitchA-vlan13] quit
[SwitchA] interface ethernet 1/7
[SwitchA-Ethernet1/7] port link-type trunk
[SwitchA-Ethernet1/7] port trunk permit vlan 11 to 13
Please wait... Done.

3. Configure Switch B:
   <SwitchB> system-view
   [SwitchB] interface ethernet 1/2
   [SwitchB-Ethernet1/2] port link-type trunk
   [SwitchB-Ethernet1/2] port trunk permit vlan 11 to 13 100
   Please wait... Done.
   [SwitchB-Ethernet1/2] qinq enable
   [SwitchB-Ethernet1/2] qinq vid 100
   [SwitchB-Ethernet1/2-vid-100] raw-vlan-id inbound 11 to 13
   [SwitchB-Ethernet1/2-vid-100] quit
   [SwitchB-Ethernet1/2] quit
   [SwitchB-Ethernet1/1] port link-type trunk
   [SwitchB-Ethernet1/1] port trunk permit vlan 100

4. Configure the router:
   # Create Ethernet subinterface GigabitEthernet 2/1/7.100 and enter subinterface view. Assign an IP address to the subinterface. Configure the subinterface to terminate QinQ packets whose inner VLAN ID is 11, 12, or 13, and outer VLAN ID is 100.
   <Router> system-view
   [Router] interface gigabitethernet 2/1/7.100
   [Router-GigabitEthernet2/1/7.100] ip address 1.1.1.11 255.255.255.0
   [Router-GigabitEthernet2/1/7.100] second-dot1q 11 to 13
   [Router-GigabitEthernet2/1/7.100] quit
   [Router-GigabitEthernet2/1/7.100] quit
   [Router-GigabitEthernet2/1/6] ip address 1.1.2.11 255.255.255.0

5. Configure Switch C:
   Use Switch C's factory configuration.

6. Configure the server group:
   Assign IP addresses in the same network segment 1.1.2.0/24 to all devices in the server group, and configure the gateway IP address as 1.1.2.11/24.
Configuration example for QinQ termination supporting DHCP relay

Network requirements

As shown in Figure 51:

- Provider A and Provider B are routers on the service provider network.
- DHCP client A and DHCP client B are routers on the customer networks.
- Provider A is the DHCP relay agent and Provider B is the DHCP server.
- Provider A and Provider B communicate with each other through Layer 3 interfaces.

The expected results after the configuration are:

- DHCP relay agent Provider A receives double-tagged packets sent from DHCP clients, terminates these QinQ packets by removing their inner and outer VLAN tags, and forwards the packets to DHCP server Provider B via the service provider network.
- DHCP client A and client B can apply for IP addresses and related network configuration parameters from Provider B via the service provider network.

Figure 51 Network diagram

Configuration procedure

1. Configure DHCP relay agent Provider A:
   # Enable DHCP.
   <ProviderA> system-view
   [ProviderA] dhcp enable
   # Create the DHCP server group.
   [ProviderA] dhcp relay server-group 1 ip 10.2.1.1
   # Create a Layer 3 Ethernet subinterface GigabitEthernet 2/1/7.100.
Configure Switch A:

# Configure uplink port Ethernet 1/1.
<SwitchA> system-view
[SwitchA] interface ethernet 1/1
[SwitchA-Ethernet1/1] port link-type trunk
# Configure Ethernet 1/1 as a trunk port and assign it to VLAN 100.
[SwitchA-Ethernet1/1] port trunk permit vlan 100
[SwitchA-Ethernet1/1] quit
# Configure downlink port Ethernet 1/2.
[SwitchA] interface ethernet 1/2
132

[SwatchA-Ethernet1/2] qinq enable
[SwatchA-Ethernet1/2] quit

# Configure downlink port Ethernet 1/3.
[SwatchA] interface Ethernet 1/3
[SwatchA-Ethernet1/3] qinq enable
[SwatchA-Ethernet1/3] quit

# Assign downlink ports Ethernet 1/2 and Ethernet 1/3 to VLAN 100.
[SwatchA] vlan 100
[SwatchA-vlan100] port ethernet 1/2
[SwatchA-vlan100] port ethernet 1/3

4. Configure Switch B:

# Assign port Ethernet 1/2 to VLAN 20.
<SwitchB> system-view
[SwatchB] vlan 20
[SwatchB-vlan20] port ethernet 1/2
[SwatchB-vlan20] quit

# Configure port Ethernet 1/1 as a trunk port and assign it to VLAN 20.
[SwatchB] interface ethernet 1/1
[SwatchB-Ethernet1/1] port link-type trunk
[SwatchB-Ethernet1/1] port trunk permit vlan 20

5. Configure Switch C:

# Assign port Ethernet 1/2 to VLAN 10.
<SwitchC> system-view
[SwatchC] vlan 10
[SwatchC-vlan10] port ethernet 1/2
[SwatchC-vlan10] quit

# Configure Ethernet 1/1 as a trunk port and assign it to VLAN 10.
[SwatchC] interface ethernet 1/1
[SwatchC-Ethernet1/1] port link-type trunk
[SwatchC-Ethernet1/1] port trunk permit vlan 10
Configuring LLDP

Overview

Background

In a heterogeneous network, it is important that different types of devices from different vendors can discover one another and exchange configuration for interoperability and management sake. This calls for a standard configuration exchange platform.

To address this need, the IETF drafted the Link Layer Discovery Protocol (LLDP) in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a network device sends local device information (including its major functions, management IP address, device ID, and port ID) as TLV (type, length, and value) triplets in LLDPDUs to the directly connected network devices, and at the same time, stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB). This allows a network management system to quickly detect and identify the Layer-2 network topology change.

NOTE:
For more information about MIBs, see Network Management and Monitoring Configuration Guide.

Basic concepts

LLDP frames

LLDP sends device information in LLDP data units (LLDPDUs). LLDPDUs are encapsulated in Ethernet II or SNAP frames.

1. Ethernet II-encapsulated LLDP frame format

Figure 52 Ethernet II-encapsulated LLDP frame format
Table 19 Fields in an Ethernet II-encapsulated LLDP frame

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination MAC address</td>
<td>The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.</td>
</tr>
<tr>
<td>Type</td>
<td>The Ethernet type for the upper layer protocol. It is 0x88CC for LLDP.</td>
</tr>
<tr>
<td>Data</td>
<td>LLDP data unit (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>

2. SNAP-encapsulated LLDP frame format

Figure 53 SNAP-encapsulated LLDP frame format

Table 20 Fields in a SNAP-encapsulated LLDP frame

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination MAC address</td>
<td>The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.</td>
</tr>
<tr>
<td>Type</td>
<td>The SNAP type for the upper layer protocol. It 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>

LLDPDUs

LLDP uses LLDPDUs to exchange information. An LLDPDU comprises multiple TLV sequences, each carrying a type of device information, as shown in Figure 54.

Figure 54 Mandatory and optional TLVs in an LLDPDU

<table>
<thead>
<tr>
<th>Chassis ID TLV</th>
<th>Port ID TLV</th>
<th>TTL TLV</th>
<th>Optional TLV</th>
<th>Optional TLV</th>
<th>End TLV</th>
</tr>
</thead>
</table>
An LLDPDU can carry up to 28 types of TLVs. The chassis ID TLV, port ID TLV, TTL TLV, and end of LLDPDU TLV (end TLV in the figure) are mandatory TLVs that must be carried. Other TLVs are optional.

**TLVs**

TLVs are type, length, and value sequences that carry information elements, where the type field identifies the type of information, the length field indicates the length of the information field in octets, and the value field contains the information itself.

LLDPDU TLVs fall into 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, and are defined by standardization or other organizations and thus are optional to LLDPDUs.

1. **Basic management TLVs**

   Table 19 lists the basic management TLV types. Some of them are mandatory to LLDPDUs, and must be included in every LLDPDU.

   **Table 21 Basic LLDP TLVs**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID</td>
<td>Bridge MAC address of the sending device</td>
<td></td>
</tr>
<tr>
<td>Port ID</td>
<td>ID of the sending port.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If MED TLVs are included in the LLDPDU, the port ID TLV carries</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>the MAC address of the sending port or the bridge MAC in case the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port does not have a MAC address. If no MED TLVs are included,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the port ID TLV carries the port name.</td>
<td></td>
</tr>
<tr>
<td>Time To Live</td>
<td>Life of the transmitted information on the receiving device</td>
<td></td>
</tr>
<tr>
<td>End of LLDPDU</td>
<td>Marks the end of the TLV sequence in the LLDPDU</td>
<td></td>
</tr>
<tr>
<td>Port Description</td>
<td>Port description of the sending port</td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>Name of the sending device</td>
<td></td>
</tr>
<tr>
<td>System Description</td>
<td>Description of the sending device</td>
<td></td>
</tr>
<tr>
<td>System Capabilities</td>
<td>Identifies the primary functions of the sending device and the</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>primary functions that have been enabled</td>
<td></td>
</tr>
<tr>
<td>Management Address</td>
<td>Management address used to reach higher level entities to assist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discovery by network management, and the interface number and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>object identifier (OID) associated with the address</td>
<td></td>
</tr>
</tbody>
</table>

2. **IEEE 802.1 organizationally specific TLVs**

   **Table 22 IEEE 802.1 organizationally specific TLVs**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port VLAN ID</td>
<td>PVID of the sending port</td>
</tr>
<tr>
<td>Port And Protocol VLAN ID</td>
<td>Port and protocol VLAN IDs</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>A specific VLAN name on the port</td>
</tr>
</tbody>
</table>
**NOTE:**
H3C routers support receiving but not sending protocol identity TLVs.

### 3. IEEE 802.3 organizationally specific TLVs

**Table 23 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 rate and duplex capabilities of the sending port, support for auto negotiation, enabling status of auto negotiation, and the current rate and duplex mode.</td>
</tr>
<tr>
<td>Power Via MDI</td>
<td>Contains Power supply capability of the port.</td>
</tr>
<tr>
<td>Link Aggregation</td>
<td>Indicates the support of the port for link aggregation, the aggregation capability of the port, and the aggregation status (that is, whether the link is in an aggregation).</td>
</tr>
<tr>
<td>Maximum Frame Size</td>
<td>Indicates the supported maximum frame size. It is now the MTU of the port.</td>
</tr>
</tbody>
</table>

### 4. 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 satisfy the voice device vendors’ requirements for cost effectiveness, ease of deployment, and ease of management. In addition, LLDP-MED TLVs make deploying voice devices in Ethernet easier. LLDP-MED TLVs are shown in Table 24.

**Table 24 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 it supports.</td>
</tr>
<tr>
<td>Network Policy</td>
<td>Allows a network device or terminal device to advertise VLAN ID of the specific port, 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 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 that the user specifies the asset ID for the endpoint to facilitate directory management and asset tracking.</td>
</tr>
<tr>
<td>Location Identification</td>
<td>Allows a network device to advertise the appropriate location identifier information for a terminal device to use in the context of location-based applications.</td>
</tr>
</tbody>
</table>
Management address

The management address of a network device is used by the network management system to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

How LLDP works

Operating Modes of LLDP

LLDP can operate in one of the following modes:

- **TxRx mode**—A port in this mode sends and receives LLDP frames.
- **Tx mode**—A port in this mode only sends LLDP frames.
- **Rx mode**—A port in this mode only receives LLDP frames.
- **Disable mode**—A port in this mode does not send or receive LLDP frames.

Each time the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. An initialization delay, which is user configurable, prevents LLDP from being initialized too frequently at times of frequent operating mode change. With this delay configured, before a port can initialize LLDP, it must wait for the specified interval after the LLDP operating mode changes.

Transmitting LLDP frames

An LLDP-enabled port operating in TxRx mode or Tx mode sends LLDP frames to its directly connected network devices both periodically and when the local configuration changes. A frame transmit interval between two successive LLDP frames prevents the network from being overwhelmed by LLDP frames at times of frequent local device information change.

This interval is shortened to 1 second in either of the following cases:

- A new LLDP frame is received carrying device information new to the local device.
- The LLDP operating mode of the port changes from Disable/Rx to TxRx or Tx.

This is the fast sending mechanism of LLDP. With this mechanism, a specific number of LLDP frames are sent successively at the 1-second interval to help LLDP neighbors discover the local device as soon as possible. Then, the normal LLDP frame transmit interval resumes.

Receiving LLDP frames

An LLDP-enabled port operating in TxRx mode or Rx mode checks the TLVs carried in every LLDP frame it receives for validity violation. If valid, the information is saved and an aging timer is set for it based on the time to live (TTL) TLV carried in the LLDPDU. If the TTL TLV is zero, the information is aged out immediately.

Protocols and standards

The protocols and standards related to LLDP include:

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*

LLDP configuration task list

Complete these tasks to configure LLDP:
Performing basic LLDP configuration

Enabling LLDP

To make LLDP take effect on specific ports, you must enable LLDP both globally and on these ports.

To enable LLDP on the router:

<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 LLDP globally.</td>
<td>lldp enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Ethernet interface view or port group view.</td>
<td>• Enter Layer 2 or Layer 3 Ethernet interface view: interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter port group view: port-group manual port-group-name</td>
</tr>
<tr>
<td>4.</td>
<td>Enable LLDP.</td>
<td>lldp enable</td>
</tr>
</tbody>
</table>

Setting LLDP operating mode

LLDP can operate in one of the following modes:
- **TxRx mode** — A port in this mode sends and receives LLDPDUs.
• **Tx mode**—A port in this mode only sends LLDPDUs.
• **Rx mode**—A port in this mode only receives LLDPDUs.
• **Disable mode**—A port in this mode does not send or receive LLDPDUs.

To set the LLDP operating 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 Ethernet interface view or port group view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 or Layer 3 Ethernet interface view:</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td>port-group manual port-group-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the LLDP operating mode.</td>
<td>lldp admin-status { disable</td>
</tr>
</tbody>
</table>

The default setting is TxRx.

### Setting the LLDP re-initialization delay

When the LLDP operating mode changes on a port, the port initializes the protocol state machines after a LLDP re-initialization delay. By adjusting the LLDP re-initialization delay, you can avoid frequent initializations caused by frequent LLDP operating mode changes on a port.

To set the LLDP re-initialization delay for 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>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the LLDP re-initialization delay.</td>
<td>lldp timer reinit-delay delay</td>
</tr>
</tbody>
</table>

The default setting is 2 seconds.

### Enable LLDP polling

With LLDP polling enabled, the router periodically checks for local configuration changes. On detecting a configuration change, the router sends LLDPDUs to inform neighboring routers of the change.

To enable LLDP polling on the specified port or 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>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view or port group view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 or Layer 3 Ethernet interface view:</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>• Enter port group view:</td>
<td>port-group manual port-group-name</td>
</tr>
</tbody>
</table>
3. Enable LLDP polling and set the polling interval.

   **lldp check-change-interval interval**

   By default, LLDP polling is disabled.

---

### Configuring the advertisable TLVs

To configure the advertisable LLDPDU TLVs on the specified port or ports:

1. Enter system view.

   **system-view**

   N/A

2. Enter Ethernet interface view or port group view.

   - Enter Layer 2 or Layer 3 Ethernet interface view:
     
     ```
     interface interface-type interface-number
     ```

   - Enter port group view:
     
     ```
     port-group manual port-group-name
     ```

3. Configure the advertisable TLVs (Layer 2 Ethernet interface view or port group view).

   ```
   lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id { vlan-id | vlan-name { vlan-id } } | dot3-tlv { all | link-aggregation | mac-physical | max-frame-size | power | med-tlv { all | capability | inventory | location-id { civic-address device-type country-code { ca-type ca-value }&<1-10> | elin-address tel-number } | network-policy | power-over-ethernet } }
   ```

   Optional.

   By default, all types of LLDP TLVs except location identification TLVs are advertisable on a Layer 2 Ethernet port.

4. Configure the advertisable TLVs (Layer 3 Ethernet interface view).

   ```
   lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name } | dot3-tlv { all | link-aggregation | mac-physical | max-frame-size | power | med-tlv { all | capability | inventory | location-id { civic-address device-type country-code { ca-type ca-value }&<1-10> | elin-address tel-number } | network-policy | power-over-ethernet } }
   ```

   Optional.

   By default, all types of LLDP TLVs, except IEEE 802.1 organizationally specific TLVs, network policy TLVs, and location identification TLVs, are advertisable on a Layer 3 Ethernet port.

---

### Configuring the management address and its encoding format

LLDP encodes the management address in numeric or character string format in management address TLVs.

By default, management addresses are encoded in numeric format. If a neighbor encodes its management address in character string format, you must configure the encoding format of the management address as string on the connecting port to guarantee normal communication with the neighbor.
To configure the management address to be advertised and its encoding format on a port or a group of 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>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter Ethernet interface view or port group view. | • Enter Layer 2 or Layer 3 Ethernet interface view:  
  interface interface-type interface-number  
  • Enter port group view:  
  port-group manual  
  port-group-name | Use either command. |
| 3.   | Allow LLDP to advertise the management address in LLDPDUs and configure the advertised management address. | lldp management-address-tlv [ ip-address ] | Optional.  
By default, the management address is sent through LLDPDUs.  
• For a Layer 2 Ethernet port, the management address is the main IP address of the lowest-ID VLAN carried on the port. If none of the carried VLANs is assigned an IP address, no management address will be advertised.  
• For a Layer 3 Ethernet port, the management address is its own IP address. If no IP address is configured for the Layer 3 Ethernet port, no management address will be advertised. |
| 4.   | Configure the encoding format of the management address as character string. | lldp management-address-format string | By default, the management address is encoded in the numeric format. |

Setting other LLDP parameters

The Time To Live TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can configure the TTL of locally sent LLDPDUs, which determines how long information about the local router can be saved on a neighboring router. The TTL is expressed using the following formula:

\[
\text{TTL TLV} = \text{TTL multiplier} \times \text{LLDPDU transmit interval}
\]

To set related LLDP 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>
</tbody>
</table>
| 2.   | Set the TTL multiplier. | lldp hold-multiplier value | Optional.  
The default setting is 4. |
### Configuring the encapsulation format for LLDPDUs

LLDPDUs can be encapsulated in Ethernet II or SNAP frames.

- With Ethernet II encapsulation configured, an LLDP port sends LLDPDUs in Ethernet II frames and processes an incoming LLDP frame only when it is Ethernet II encapsulated.
- With SNAP encapsulation configured, an LLDP port sends LLDPDUs in SNAP frames and processes an incoming LLDP frame only when it is SNAP encapsulated.

By default, LLDPDUs are encapsulated in Ethernet II frames. If the neighbor routers encapsulate LLDPDUs in SNAP frames, configure the encapsulation format for LLDPDUs as SNAP to guarantee normal communication with the neighbors.

To configure the encapsulation format for LLDPDUs:

<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 Ethernet interface view or port group view.</td>
<td>Use either command.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the encapsulation format for LLDPDUs as SNAP.</td>
<td>Ethernet II encapsulation format applies by default.</td>
</tr>
</tbody>
</table>
Configuring CDP compatibility

To make your router work with Cisco IP phones, you must enable CDP compatibility.

With CDP compatibility enabled, your router can receive and recognize CDP packets from a Cisco IP phone and respond with CDP packets.

Configuration prerequisites

Before configuring CDP compatibility, perform the following configurations:

- Enable LLDP globally.
- Enable LLDP on the port connected to an IP phone and configure LLDP to operate in TxRx mode on the port.

Configuring CDP compatibility

CDP-compatible LLDP operates in one of the follows modes:

- **TxRx**—CDP packets can be transmitted and received.
- **Disable**—CDP packets can be neither transmitted nor received.

To make CDP-compatible LLDP take effect on specific ports, first enable CDP-compatible LLDP globally, and then configure CDP-compatible LLDP to operate in TxRx mode.

To enable 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>N/A</td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enable CDP compatibility globally.</td>
<td>lldp compliance cdp</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Ethernet interface view or port group view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter Layer 2 or Layer 3 Ethernet interface view: interface interface-type interface-number</td>
<td>Use either command.</td>
</tr>
<tr>
<td></td>
<td>• Enter port group view: port-group manual port-group-name</td>
<td></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>
</tbody>
</table>

⚠️ CAUTION:

The maximum TTL value allowed by CDP is 255 seconds. To make CDP-compatible LLDP work properly with Cisco IP phones, make sure that the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds.

Configuring LLDP trapping

LLDP trapping notifies the network management system (NMS) of events such as newly-detected neighboring devices and link malfunctions.
LLDP traps are sent periodically, and the trap transmit interval is configurable. In response to topology changes detected, the router sends LLDP traps according to the interval configured to inform the neighboring routers of the changes.

To configure LLDP 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 Ethernet interface view or port group view.</td>
<td>• Enter Layer 2 or Layer 3 Ethernet interface view: interface interface-type interface-number&lt;br&gt;• Enter port group view: port-group manual port-group-name</td>
</tr>
<tr>
<td>3.</td>
<td>Enable LLDP trapping.</td>
<td>lldp notification remote-change enable</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Set the LLDP transmit interval.</td>
<td>lldp timer notification-interval interval</td>
</tr>
</tbody>
</table>

### Displaying and maintaining LLDP

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the global LLDP information or the information contained in the LLDP TLVs to be sent through a port.</td>
<td>display lldp local-information [ global</td>
<td>interface interface-type interface-number ] [</td>
</tr>
<tr>
<td>Display the information contained in the LLDP TLVs sent from neighboring routers.</td>
<td>display lldp neighbor-information [ brief</td>
<td>interface interface-type interface-number [ brief ]</td>
</tr>
<tr>
<td>Display LLDP statistics.</td>
<td>display lldp statistics [ global</td>
<td>interface interface-type interface-number ] [</td>
</tr>
<tr>
<td>Display LLDP status of a port.</td>
<td>display lldp status [ interface interface-type interface-number ] [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display types of advertisable optional LLDP TLVs.</td>
<td>display lldp tlv-config [ interface interface-type interface-number ] [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>
LLDP configuration examples

Basic LLDP configuration example

Network requirements

As shown in Figure 55, the NMS and Router A are located in the same Ethernet. Enable LLDP on the ports of Router A and Router B to monitor the link between Router A and Router B and the link between Router A and the MED device on the NMS.

Figure 55 Network diagram

![Network diagram]

Configuration procedure

1. Configure Router A:
   
   # Enable LLDP globally.
   
   `<RouterA> system-view
   [RouterA] lldp enable
   
   # Enable LLDP on GigabitEthernet 4/1/1 and GigabitEthernet 4/1/2 (you can skip this step because LLDP is enabled on ports by default), and set the LLDP operating mode to Rx.

   `[RouterA-GigabitEthernet4/1/1] interface gigabitethernet 4/1/1
   [RouterA-GigabitEthernet4/1/1] lldp enable
   [RouterA-GigabitEthernet4/1/1] lldp admin-status rx
   [RouterA-GigabitEthernet4/1/1] quit

   `[RouterA-GigabitEthernet4/1/2] interface gigabitethernet 4/1/2
   [RouterA-GigabitEthernet4/1/2] lldp enable
   [RouterA-GigabitEthernet4/1/2] lldp admin-status rx
   [RouterA-GigabitEthernet4/1/2] quit

2. Configure Router B:

   # Enable LLDP globally.

   `<RouterB> system-view
   [RouterB] lldp enable
   
   # Enable LLDP on GigabitEthernet 4/1/1 (you can skip this step because LLDP is enabled on ports by default), and set the LLDP operating mode to Tx.

   `[RouterB] interface gigabitethernet 4/1/1
   [RouterB-GigabitEthernet4/1/1] lldp enable
   [RouterB-GigabitEthernet4/1/1] lldp admin-status tx
   [RouterB-GigabitEthernet4/1/1] quit
3. Verify the configuration:

# Display the global LLDP status and port LLDP status on Router A.

[RouterA] display lldp status
Global status of LLDP : Enable
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
Hold multiplier : 4
Reinit delay : 2s
Transmit delay : 2s
Trap interval : 5s
Fast start times : 3

Port 1 [GigabitEthernet4/1/1]:
Port status of LLDP : Enable
Admin status : Rx Only
Trap flag : No
Polling interval : 0s

Number of neighbors : 1
Number of MED neighbors : 1
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0

Port 2 [GigabitEthernet4/1/2]:
Port status of LLDP : Enable
Admin status : Rx Only
Trap flag : No
Polling interval : 0s

Number of neighbors : 1
Number of MED neighbors : 0
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 3

The output shows that: GigabitEthernet 4/1/1 of Router A connects a MED device, and GigabitEthernet 4/1/2 of Router A connects a non-MED device. Both ports operate in Rx mode, in other words, they only receive LLDP frames.

# Tear down the link between Router A and Router B and then display the global LLDP status and port LLDP status on Router A.

[RouterA] 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
Hold multiplier : 4
Reinit delay : 2s
Transmit delay : 2s
Trap interval : 5s
Fast start times : 3

Port 1 [GigabitEthernet4/1/1]:
Port status of LLDP : Enable
Admin status : Rx_Only
Trap flag : No
Polling interval : 0s

Number of neighbors : 1
Number of MED neighbors : 1
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 5

Port 2 [GigabitEthernet4/1/2]:
Port status of LLDP : Enable
Admin status : Rx_Only
Trap flag : No
Polling interval : 0s

Number of neighbors : 0
Number of MED neighbors : 0
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0

The output shows that GigabitEthernet 4/1/2 of Router A does not connect any neighboring router.

CDP-compatible LLDP configuration example

Network requirements

As shown in Figure 56, enable CDP compatibility of LLDP on Router A.

Figure 56 Network diagram

![Network diagram](image)

Configuration procedure

1. Configure CDP-compatible LLDP on Router A:

   # Enable LLDP globally and enable LLDP to be compatible with CDP globally.
   [RouterA] lldp enable
   [RouterA] lldp compliance cdp
# Enable LLDP (you can skip this step because LLDP is enabled on ports by default), configure LLDP to operate in TxRx mode, and configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 4/1/1 and GigabitEthernet 4/1/2.

[RouterA] interface gigabitethernet 4/1/1
[RouterA-GigabitEthernet4/1/1] lldp enable
[RouterA-GigabitEthernet4/1/1] lldp admin-status txrx
[RouterA-GigabitEthernet4/1/1] lldp compliance admin-status cdp txrx
[RouterA-GigabitEthernet4/1/1] quit

[RouterA] interface gigabitethernet 4/1/2
[RouterA-GigabitEthernet4/1/2] lldp enable
[RouterA-GigabitEthernet4/1/2] lldp admin-status txrx
[RouterA-GigabitEthernet4/1/2] lldp compliance admin-status cdp txrx
[RouterA-GigabitEthernet4/1/2] quit

2. Verify the configuration:

# Display the neighbor information on Router A.
[RouterA] display lldp neighbor-information

CDP neighbor-information of port 1[GigabitEthernet4/1/1]:
  CDP neighbor index : 1
  Chassis ID : SEP00141CBCDBFE
  Port ID : Port 1
  Software version : P0030301MFG2
  Platform : Cisco IP Phone 7960
  Duplex : Full

CDP neighbor-information of port 2[GigabitEthernet4/1/2]:
  CDP neighbor index : 2
  Chassis ID : SEP00141CDBDFE
  Port ID : Port 1
  Software version : P0030301MFG2
  Platform : Cisco IP Phone 7960
  Duplex : Full

The output shows that Router A has discovered the IP phones connected to GigabitEthernet 4/1/1 and GigabitEthernet 4/1/2, and has obtained their LLDP device information.
Index

B  
BPDU tunneling configuration example, 105

C  
Configure basic settings of a VLAN interface, 4
Configuring an aggregate interface, 79
Configuring an aggregation group, 74
Configuring an isolation group, 92
Configuring basic VLAN settings, 3
Configuring BPDU tunneling, 104
Configuring GARP timers, 112
Configuring GVRP functions, 111
Configuring load sharing criteria for link aggregation groups, 83
Configuring the MAC address table, 20
Configuring the spanning tree, 41
Configuring TPID for VLAN-tagged packets, 121

D  
Displaying and maintaining Ethernet link aggregation, 83
Displaying and maintaining GVRP, 113
Displaying and maintaining isolation groups, 93
Displaying and maintaining MAC address tables, 24
Displaying and maintaining the spanning tree, 62

E  
Enabling a QinQ termination-enabled interface/subinterface to transmit broadcast and multicast packets, 124
Ethernet link aggregation configuration examples, 84
Ethernet link aggregation configuration task list, 74

G  
GVRP configuration examples, 114
GVRP configuration task list, 111

I  
Introduction to BPDU tunneling, 102
Introduction to GVRP, 107
Introduction to port isolation, 91
Introduction to QinQ, 95
Introduction to VLAN, 1

L  
LLDP configuration task list, 137

M  
MAC address table configuration example, 24
MSTP, 33
MSTP configuration example, 63

O  
Overview, 133
Overview, 19
Overview, 119
Overview, 67

P  
Performing basic LLDP configuration, 138
Port isolation configuration example, 93
Protocols and standards, 38

R  
RSTP, 33

S  
Spanning tree configuration task list, 38
STP, 26

V  
VLAN termination configuration task list, 121