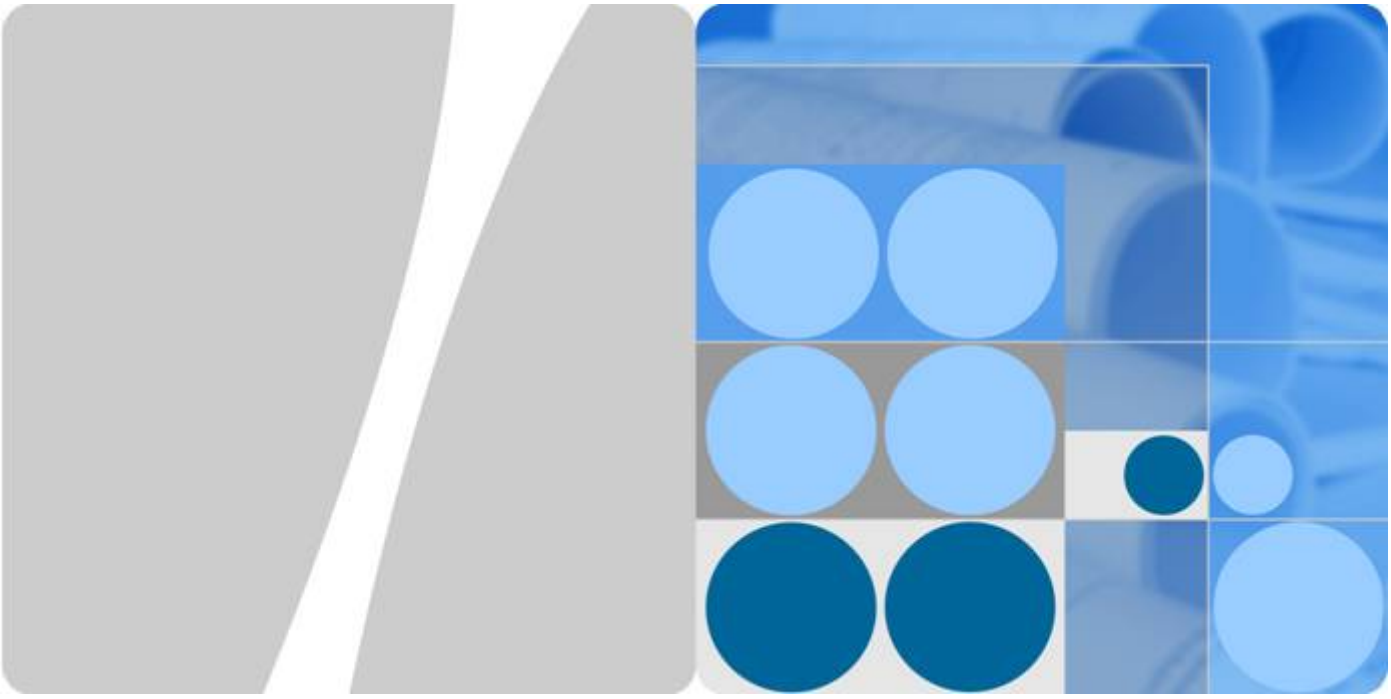


Quidway S6700 Series Ethernet Switches

V100R006C00

Typical Configuration Examples

Issue 01

Date 2011-07-15

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
Quidway S6700	V100R006C00

This document provides the typical configuration examples supported by the S6700 device.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions (Optional)

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 01 (2011-07-15)

Initial commercial release.

Contents

1 Configuration Guide - Ethernet

About This Chapter

This document describes the configuration of Ethernet services, including Ethernet interfaces, link aggregation, VLANs, VLAN mapping, QinQ, GVRP, MAC address table, STP/RSTP, MSTP, SEP, transparent transmission of Layer 2 protocol packets, and loopback detection.

The document provides the configuration procedures and configuration examples to illustrate the service configuration methods and application scenario.

1.1 Ethernet Interface Configuration
This chapter describes the basic knowledge, methods, and examples for configuring the Ethernet interface.

1.2 Link Aggregation Configuration
This chapter describes the concepts, configuration procedures, and configuration examples of link aggregation.

1.3 VLAN Configuration
Virtual Local Area Networks (VLANs) have advantages of broadcast domain isolation, security enhancement, flexible networking, and good extensibility.

1.4 VLAN Mapping Configuration
This chapter describes the basic knowledge, methods, and examples for configuring VLAN mapping.

1.5 QinQ Configuration
This chapter describes the basic knowledge, methods, and examples for configuring QinQ.

1.6 GVRP Configuration
This chapter describes basic concepts involved in GVRP, GVRP configuration procedures, and concludes with a GVRP configuration example.

1.7 MAC Address Table Configuration
This chapter provides the basics for MAC address table configuration, configuration procedure, and configuration examples.

1.8 STP/RSTP Configuration
The Spanning Tree Protocol (STP) trims a ring network into a loop-free tree network. It prevents replication and circular propagation of packets, provides multiple redundant paths for Virtual LAN (VLAN) data traffic, and enables load balancing. The Rapid Spanning Tree Protocol

(RSTP) develops rapid convergence and introduces the edge port and its protection function based on STP.

1.9 MSTP Configuration

The Multiple Spanning Tree Protocol (MSTP) trims a ring network into a loop-free tree network. It prevents replication and circular propagation of packets, provides multiple redundant paths for Virtual LAN (VLAN) data traffic, and enables load balancing.

1.10 SEP Configuration

As a link layer protocol dedicated to Ethernet rings, SEP blocks redundant links on a network to prevent logical loops.

1.11 Layer 2 Protocol Transparent Transmission Configuration

This chapter describes the concept, configuration procedure, and configuration examples of Layer 2 protocol transparent transmission.

1.1 Ethernet Interface Configuration

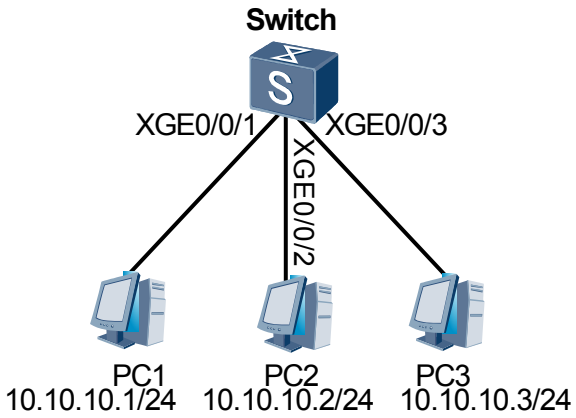
This chapter describes the basic knowledge, methods, and examples for configuring the Ethernet interface.

1.1.1 Example for Configuring Port Isolation

Networking Requirements

As shown in **Figure 1-1**, it is required that PC1 and PC2 cannot communicate with each other, but they can communicate with PC3.

Figure 1-1 Networking diagram for configuring port isolation



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable port isolation on the ports connected to PC1 and PC2 respectively to prevent PC1 and PC2 from communicating with each other.

Data Preparation

To complete the configuration, you need the following data:

- Number of the port connected to PC1
- Number of the port connected to PC2
- Port isolation mode: Layer 2 isolation and Layer 3 communication (default configuration)
- ID of the VLAN that the ports connected to PC1, PC2, and PC3 belong to (VLAN 1 by default)
- Port isolation group that the ports connected to PC1 and PC2 belong to (group 1 by default)

Procedure

Step 1 Enable port isolation.

Isolate ports on Layer 2 and allow them to communicate on Layer 3.

```
<Quidway> system-view
[Quidway] port-isolate mode l2
```

Enable port isolation on XGigabitEthernet 0/0/1.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port-isolate enable
[Quidway-XGigabitEthernet0/0/1] quit
```

Enable port isolation on XGigabitEthernet 0/0/2.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port-isolate enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 Verify the configuration.

PC1 and PC2 cannot ping each other.

PC1 and PC3 can ping each other.

PC2 and PC3 can ping each other.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
interface XGigabitEthernet0/0/1
 port-isolate enable group 1
#
interface XGigabitEthernet0/0/2
 port-isolate enable group 1
#
interface XGigabitEthernet0/0/3
#
return
```

1.2 Link Aggregation Configuration

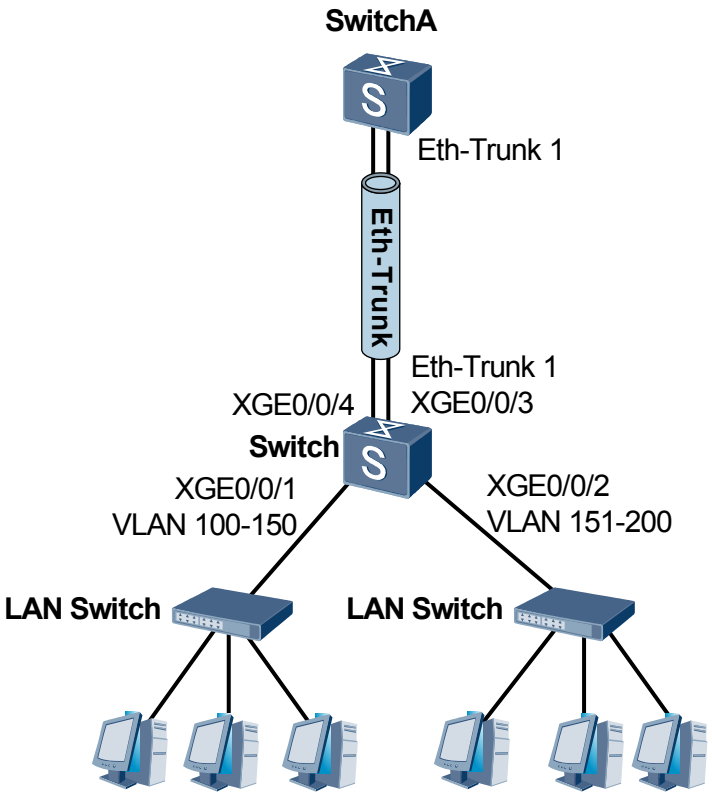
This chapter describes the concepts, configuration procedures, and configuration examples of link aggregation.

1.2.1 Example for Configuring Link Aggregation in Manual Load Balancing Mode

Networking Requirements

As shown in **Figure 1-2**, the Switch is connected to the SwitchA through an Eth-Trunk. The link between the Switch and SwitchA must ensure high reliability.

Figure 1-2 Networking diagram for configuring link aggregation in manual load balancing mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create an Eth-Trunk.
2. Add member interfaces to the Eth-Trunk.

Data Preparation

To complete the configuration, you need the following data:

- Number of the Eth-Trunk
- Types and numbers of the member interfaces in the Eth-Trunk

Procedure

Step 1 Create an Eth-Trunk.

Create Eth-Trunk 1.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] interface eth-trunk 1
[Switch-Eth-Trunk1] quit
```

Step 2 Add member interfaces to the Eth-Trunk.

Add XGE 0/0/3 to Eth-Trunk 1.

```
[Switch] interface xgigabitethernet 0/0/3
[Switch-XGigabitEthernet0/0/3] eth-trunk 1
[Switch-XGigabitEthernet0/0/3] quit
```

Add XGE 0/0/4 to Eth-Trunk 1.

```
[Switch] interface xgigabitethernet 0/0/4
[Switch-XGigabitEthernet0/0/4] eth-trunk 1
[Switch-XGigabitEthernet0/0/4] quit
```

Step 3 Configure Eth-Trunk 1.

Configure Eth-Trunk 1 to allow packets of VLANs 100 to 200 to pass through.

```
[Switch] interface eth-trunk 1
[Switch-Eth-Trunk1] port link-type trunk
[Switch-Eth-Trunk1] port trunk allow-pass vlan 100 to 200
[Switch-Eth-Trunk1] quit
```

Step 4 Verify the configuration.

Run the **display trunkmembership** command in any view to check whether Eth-Trunk 1 is created and whether member interfaces are added.

```
[Switch] display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of UP Ports in Trunk = 2
operate status: up
Interface XGigabitEthernet0/0/3, valid, operate up, weight=1,
Interface XGigabitEthernet0/0/4, valid, operate up, weight=1,
```

Display the configuration of Eth-Trunk 1.

```
[Switch] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL          Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName                Status      Weight
XGigabitEthernet0/0/3    Up        1
XGigabitEthernet0/0/4    Up        1
```

The preceding information indicates that Eth-Trunk 1 consists of member interfaces XGE 0/0/3 and XGE 0/0/4. The member interfaces are both in Up state.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Switch
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100 to 200
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
interface XGigabitEthernet0/0/4
 eth-trunk 1
#
return
```

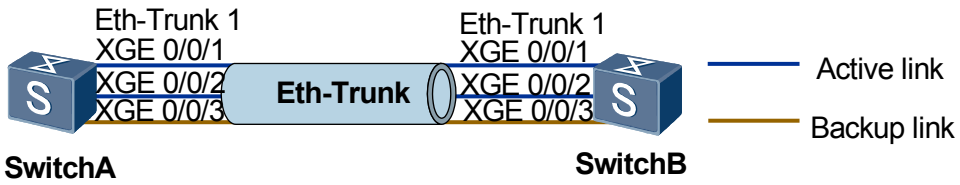
1.2.2 Example for Configuring Link Aggregation in Static LACP Mode

Networking Requirements

To improve the bandwidth and the connection reliability, configure the link aggregation group on two directly connected Switches, as shown in **Figure 1-3**. The requirements are as follows:

- M active links can implement load balancing.
- N links between two Switches can carry out redundancy backup. When a fault occurs on an active link, the backup link replaces the faulty link to keep the reliability of data transmission.

Figure 1-3 Networking diagram for configuring link aggregation in static LACP mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create an Eth-Trunk on the Switch and configure the Eth-Trunk to work in static LACP mode.
2. Add member interfaces to the Eth-Trunk.
3. Set the system priority and determine the Actor.
4. Set the upper threshold of the active interfaces.
5. Set the priority of the interface and determine the active link.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of the link aggregation groups on the Switches
- System priority of SwitchA
- Upper threshold of active interfaces
- LACP priority of the active interface

Procedure

Step 1 Create Eth-Trunk 1 and set the load balancing mode of the Eth-Trunk to static LACP mode.

Configure SwitchA.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] bpdu enable
[SwitchA-Eth-Trunk1] mode lacp-static
[SwitchA-Eth-Trunk1] quit
```

Configure SwitchB.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface eth-trunk 1
[SwitchB-Eth-Trunk1] bpdu enable
[SwitchB-Eth-Trunk1] mode lacp-static
[SwitchB-Eth-Trunk1] quit
```

Step 2 Add member interfaces to the Eth-Trunk.

Configure SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] eth-trunk 1
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] eth-trunk 1
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] eth-trunk 1
[SwitchA-XGigabitEthernet0/0/3] quit
```

Configure SwitchB.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] eth-trunk 1
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] eth-trunk 1
[SwitchB-XGigabitEthernet0/0/2] quit
[SwitchB] interface xgigabitethernet 0/0/3
[SwitchB-XGigabitEthernet0/0/3] eth-trunk 1
[SwitchB-XGigabitEthernet0/0/3] quit
```

Step 3 Set the system priority on SwitchA to 100 so that SwitchA becomes the Actor.

[SwitchA] **lacp priority 100**

Step 4 Set the upper threshold M of active interfaces on SwitchA to 2.

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] max active-linknumber 2
[SwitchA-Eth-Trunk1] quit
```

Step 5 Set the priority of the interface and determine active links on SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] lacp priority 100
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] lacp priority 100
[SwitchA-XGigabitEthernet0/0/2] quit
```

Step 6 Verify the configuration.

Check information about the Eth-Trunk of the Switches and check whether the negotiation is successful on the link.

```
[SwitchA] display eth-trunk 1
 Eth-Trunk1's state information is:
 Local:
 LAG ID: 1                 WorkingMode: STATIC
 Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
 System Priority: 100         System ID: 00e0-fca8-0417
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: Up        Number Of Up Port In Trunk: 2
 --------------------------------------------------------------------------------
 ActorPortName          Status    PortType  PortPri   PortNo PortKey   PortState
Weight
 XGigabitEthernet0/0/1   Selected  10GE      100      6145    2865     11111100
1
 XGigabitEthernet0/0/2   Selected  10GE      100      6146    2865     11111100
1
 XGigabitEthernet0/0/3   Unselect  10GE      32768    6147    2865     11100000
1

 Partner:
 --------------------------------------------------------------------------------
 PartnerPortName        SysPri    SystemID    PortPri PortNo PortKey   PortState
 XGigabitEthernet0/0/1   32768  00e0-fca6-7f85  32768     6145   2609
11111100
 XGigabitEthernet0/0/2   32768  00e0-fca6-7f85  32768     6146   2609
11111100
 XGigabitEthernet0/0/3   32768  00e0-fca6-7f85  32768     6147   2609
11110000

[SwitchB] display eth-trunk 1
 Eth-Trunk1's state information is:
 Local:
 LAG ID: 1                 WorkingMode: STATIC
 Preempt Delay: Disabled        Hash arithmetic: According to SA-XOR-DA
 System Priority: 32768         System ID: 00e0-fca6-7f85
 Least Active-linknumber: 1     Max Active-linknumber: 8
 Operate status: Up             Number Of Up Port In Trunk: 2
 --------------------------------------------------------------------------------
 ActorPortName          Status    PortType  PortPri   PortNo  PortKey   PortState
Weight
 XGigabitEthernet0/0/1 Selected  10GE       32768     6145    2609     11111100
1
 XGigabitEthernet0/0/2 Selected  10GE       32768     6146    2609     11111100
1
 XGigabitEthernet0/0/3 Unselect  10GE       32768     6147    2609     11100000
1

 Partner:
 --------------------------------------------------------------------------------
 PartnerPortName        SysPri    SystemID     PortPri  PortNo  PortKey
PortState
 XGigabitEthernet0/0/1  100    00e0-fca8-0417  100      6145     2865
11111100
```

```
 XGigabitEthernet0/0/2  100    00e0-fca8-0417  100      6146     2865
11111100
 XGigabitEthernet0/0/3  100    00e0-fca8-0417  32768    6147     2865
11110000
```

The preceding information shows that the system priority of SwitchA is 100 and it is higher than the system priority of SwitchB. Member interfaces XGE0/0/1 and XGE0/0/2 become the active interfaces and are in Selected state. Interface XGE0/0/3 is in Unselect state. M active links work in load balancing mode and N links are the backup links.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 lacp priority 100
#
interface Eth-Trunk1
 mode lacp-static
 max active-linknumber 2
#
interface XGigabitEthernet0/0/1
 eth-trunk 1
 lacp priority  100
#
interface XGigabitEthernet0/0/2
 eth-trunk 1
 lacp priority  100
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
interface Eth-Trunk1
 mode lacp-static
#
interface XGigabitEthernet0/0/1
 eth-trunk 1
#
interface XGigabitEthernet0/0/2
 eth-trunk 1
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
return
```

1.3 VLAN Configuration

Virtual Local Area Networks (VLANs) have advantages of broadcast domain isolation, security enhancement, flexible networking, and good extensibility.

1.3.1 Example for Configuring Interface-based VLANs

It is easy to divide a LAN into VLANs based on ports. After ports are added to different VLANs, users in the same VLAN can directly communicate with each other, whereas users in different VLANs cannot directly communicate with each other.

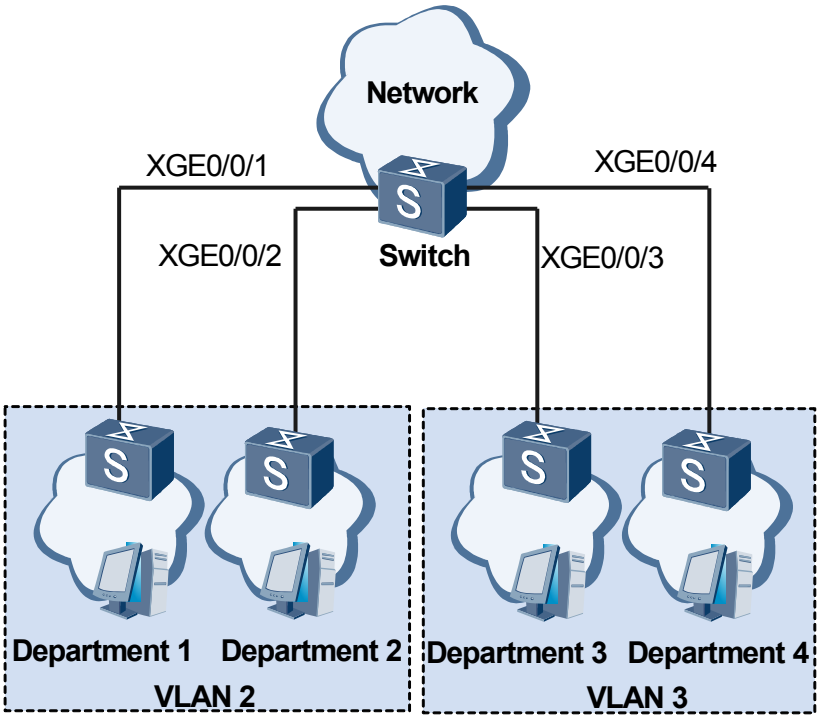
Networking Requirements

An enterprise has multiple departments. It is required that departments in charge of the same service can communicate with each other, and departments in charge of different services cannot communicate with each other.

It is required that on the network shown in **Figure 1-4**, the requirements are as follows:

- Department 1 and Department 2 are isolated from Department 3 and Department 4.
- Department 1 and Department 2 can communicate with each other.
- Department 3 and Department 4 can communicate with each other.

Figure 1-4 Networking diagram for configuring interface-based VLANs



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and determine mappings between employees and VLANs.
2. Configure port types to determine the device connected to each port.

3. Add the ports connected to department 1 and department 2 to VLAN 2 and the ports connected to department 3 and department 4 to VLAN 3 to prevent employees in department 1 or department 2 from communicating with employees in department 3 or department 4.

Data Preparation

To complete the configuration, you need the following data:

- XGE 0/0/1 and XGE 0/0/2 belong to VLAN 2.
- XGE 0/0/3 and XGE 0/0/4 belong to VLAN 3.

Procedure

Step 1 Configure the Switch.

Create VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

Set the link type of XGE 0/0/1 to trunk and add XGE 0/0/1 to VLAN 2.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type trunk
[Quidway-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
```

Set the link type of XGE 0/0/2 to trunk and add XGE 0/0/2 to VLAN 2.

```
[Quidway]interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type trunk
[Quidway-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2
[Quidway-XGigabitEthernet0/0/2] quit
```

Create VLAN 3.

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

Set the link type of XGE 0/0/3 to trunk and add XGE 0/0/3 to VLAN 3.

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] port link-type trunk
[Quidway-XGigabitEthernet0/0/3] port trunk allow-pass vlan 3
[Quidway-XGigabitEthernet0/0/3] quit
```

Set the link type of XGE 0/0/4 to trunk and add XGE 0/0/4 to VLAN 3.

```
[Quidway] interface xgigabitethernet 0/0/4
[Quidway-XGigabitEthernet0/0/4] port link-type trunk
[Quidway-XGigabitEthernet0/0/4] port trunk allow-pass vlan 3
[Quidway-XGigabitEthernet0/0/4] quit
```

Step 2 Verify the configuration.

Ping any host in VLAN 3 from a host in VLAN 2. The ping operation fails. This indicates that Department 1 and Department 2 are isolated from Department 3 and Department 4.

Ping any host in Department 2 from a host in Department 1. The ping operation is successful. This indicates that Department 1 and Department 2 can communicate with each other.

Ping any host in Department 4 from a host in Department 3. The ping operation is successful. This indicates that Department 3 and Department 4 can communicate with each other.

----End

Configuration Files

The following lists the configuration file of the Switch.

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 3
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 3
#
return
```

1.3.2 Example for Configuring MAC Address-based VLAN Assignment

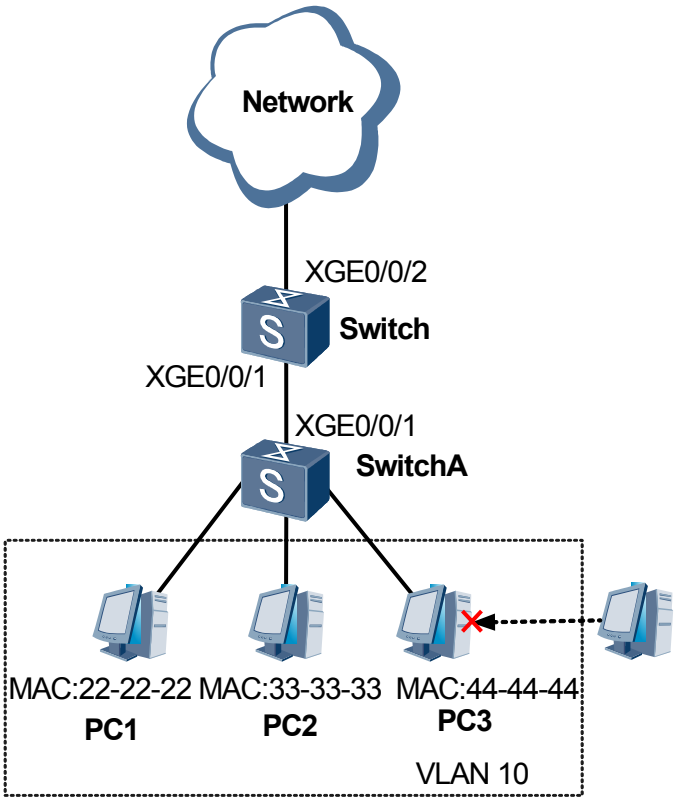
MAC address-based VLAN assignment is applicable only to simple networks where network adapters are not changed frequently.

Networking Requirements

On an enterprise network, the network administrator adds PCs of employees in a department to the same VLAN. To improve information security, only employees is this department are allowed to access the intranet.

As shown in **Figure 1-5**, only PC1, PC2, and PC3 are allowed to access the intranet through SwitchA and Switch.

Figure 1-5 Network diagram of MAC address-based VLAN assignment



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and determine the VLAN that PCs of employees belong to.
2. Add Ethernet interfaces to VLANs.
3. Associate MAC addresses of PC1, PC2, and PC3 with the specified VLAN so that the Switch can assign the VLAN to packets according to their source MAC addresses.

Data Preparation

To complete the configuration, you need the following data:

- The PVID of XGE0/0/1 on the Switch is 100.
- XGE0/0/1 of the Switch needs to be added to VLAN 10 in untagged mode.
- XGE0/0/2 of the Switch needs to be added to VLAN 10 in tagged mode.
- All the interfaces on SwitchA need to be added to VLAN 1 in untagged mode.
- MAC addresses of PC1, PC2, and PC3 need to be associated with VLAN 10.

Procedure

Step 1 Configure the Switch.

Create VLANs.

```
<Quidway> system-view
[Quidway] vlan batch 10 100
```

Set the PVID of interfaces and add interfaces to the VLANs.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid tagged vlan 10
[Quidway-XGigabitEthernet0/0/2] quit
```

Associate MAC addresses of PC1, PC2, and PC3 with VLAN 10.

```
[Quidway] vlan 10
[Quidway-Vlan10] mac-vlan mac-address 22-22-22
[Quidway-Vlan10] mac-vlan mac-address 33-33-33
[Quidway-Vlan10] mac-vlan mac-address 44-44-44
[Quidway-Vlan10] quit
```

Enable MAC address-based VLAN assignment on XGE0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] mac-vlan enable
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Verify the configuration.

PC1, PC2, and PC3 can access the intranet, whereas PCs of non-employees cannot access the intranet.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 10 100
#
vlan 10
 mac-vlan mac-address 0022-0022-0022
 mac-vlan mac-address 0033-0033-0033
 mac-vlan mac-address 0044-0044-0044
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10
#
return
```

1.3.3 Example for Configuring IP Subnet-based VLAN Assignment

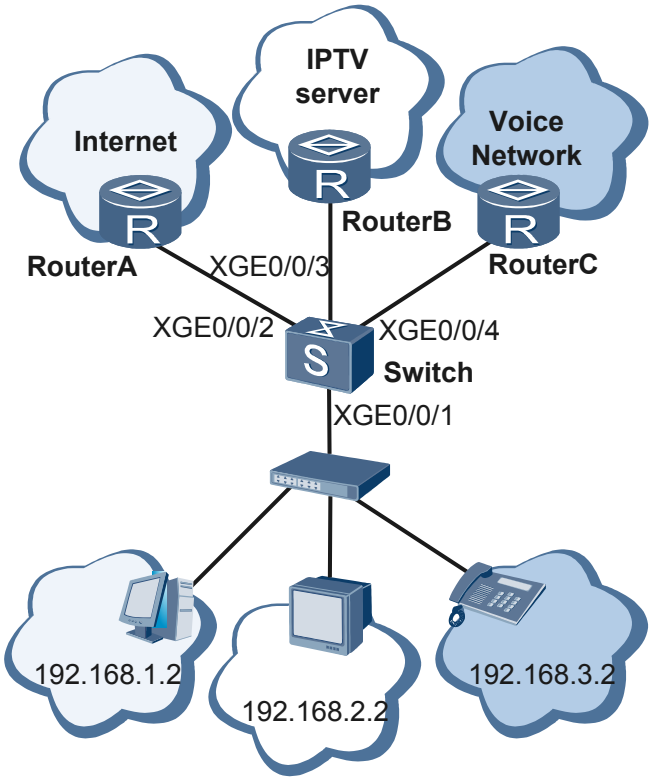
After a LAN is divided into VLANs based on IP subnets, frames from a certain network segment or IP address are transmitted in a specified VLAN. This reduces the configuration workload of network administrators and facilitates management.

Networking Requirements

A company has multiple services including the IPTV, VoIP, and Internet access services. Each service uses a unique IP address. Packets of the same service must be transmitted in the same VLAN and packets of different services must be transmitted in different VLANs.

On the network shown in **Figure 1-6**, a switch receives Internet, IPTV, and voice services from users of which IP addresses are diverse. It is required that different types of services be transmitted in separate VLANs. This allows each type of services to be sent to a remote dedicated server.

Figure 1-6 Networking diagram of IP subnet-based VLAN assignment



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and determine mappings between services and VLANs.
2. Associate IP subnets with VLANs.

   The switch determines the VLAN mapped to a frame based on the source IP address carried in the frame. New nodes can be deployed on the network without too much configuration. The switch is able to add each new node to a corresponding VLAN based on the network address of the node.
3. Configure a port to allow frames with specified VLAN IDs to pass through.
4. Configure the highest priority for IP subnet-based VLAN assignment.
5. Enable IP subnet-based VLAN assignment.

Data Preparation

To complete the configuration, you need the following data:

- VLANs to which XGE 0/0/1 needs to be added in untagged mode: VLAN 100, VLAN 200, and VLAN 300
- VLANs to which XGE 0/0/2, XGE 0/0/3, and XGE 0/0/4 need to be added in tagged mode respectively: VLAN 100, VLAN 200, and VLAN 300
- Configuration data for IP subnet-based VLAN assignment, as shown in **Table 1-1**

Table 1-1 Configuration data for IP subnet-based VLAN assignment

VLAN ID	IP Subnet Index	Source IP Address	Subnet Mask	802.1p Priority
100	1	192.168.1.2	255.255.255.0	2
200	1	192.168.2.2	255.255.255.0	3
300	1	192.168.3.2	255.255.255.0	4

Procedure

Step 1 Create VLANs.

Create VLAN 100, VLAN 200, and VLAN 300 on the Switch.

```
<Quidway> system-view
[Quidway] vlan batch 100 200 300
```

Step 2 Configure interfaces.

Set the link type of XGE 0/0/1 to hybrid and add it to VLAN 100, VLAN 200, and VLAN 300.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type hybrid
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 100 200 300
[Quidway-XGigabitEthernet0/0/1] quit
```

Add XGE 0/0/2 of the Switch to VLAN 100.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type trunk
[Quidway-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Quidway-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/3 of the Switch to VLAN 200.

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] port link-type trunk
[Quidway-XGigabitEthernet0/0/3] port trunk allow-pass vlan 200
[Quidway-XGigabitEthernet0/0/3] quit
```

Add XGE 0/0/4 of the Switch to VLAN 300.

```
[Quidway] interface xgigabitethernet 0/0/4
[Quidway-XGigabitEthernet0/0/4] port link-type trunk
[Quidway-XGigabitEthernet0/0/4] port trunk allow-pass vlan 300
[Quidway-XGigabitEthernet0/0/4] quit
```

Enable the IP subnet-based VLAN function on XGE 0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] ip-subnet-vlan enable
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 3 Configure IP subnet-based VLAN assignment.

Associate 192.168.1.2 to VLAN 100 and set the 802.1p priority of VLAN 100 to 2.

```
[Quidway] vlan 100
[Quidway-vlan100] ip-subnet-vlan 1 ip 192.168.1.2 24 priority 2
[Quidway-vlan100] quit
```

Associate 192.168.2.2 to VLAN 200 and set the 802.1p priority of VLAN 200 to 3.

```
[Quidway] vlan 200
[Quidway-vlan200] ip-subnet-vlan 1 ip 192.168.2.2 24 priority 3
[Quidway-vlan200] quit
```

Associate IP subnet 192.168.3.2 to VLAN 100 and set the 802.1p priority of VLAN 300 to 4.

```
[Quidway] vlan 300
[Quidway-vlan300] ip-subnet-vlan 1 ip 192.168.3.2 24 priority 4
[Quidway-vlan300] quit
```

Step 4 Verify the configuration.

Run the **display ip-subnet-vlan vlan all** command on the Switch. The following information is displayed:

```
[Quidway] display ip-subnet-vlan vlan all
-------------------------------------------------------------------
 Vlan    Index   IpAddress           SubnetMask          Priority
 -------------------------------------------------------------------
 100     1       192.168.1.2         255.255.255.0       2
 200     1       192.168.2.2         255.255.255.0       3
 300     1       192.168.3.2         255.255.255.0       4
 -------------------------------------------------------------------
 ip-subnet-vlan count: 3                 total count: 3
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 100 200 300
#
vlan 100
 ip-subnet-vlan 1 ip 192.168.1.2 255.255.255.0 priority 2
#
vlan 200
 ip-subnet-vlan 1 ip 192.168.2.2 255.255.255.0 priority 3
#
vlan 300
 ip-subnet-vlan 1 ip 192.168.3.2 255.255.255.0 priority 4
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 100 200 300
 ip-subnet-vlan enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
#
```

```
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 300
#
return
```

1.3.4 Example for Configuring Protocol-based VLAN Assignment

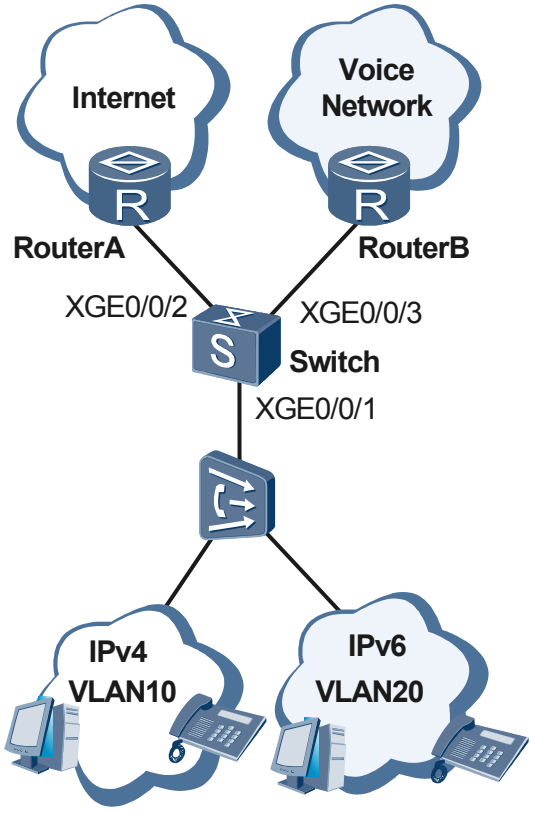
Protocol-based VLAN assignment reduces manual configuration workload and allows users to easily join a VLAN, transfer from one VLAN to another, and exit from a VLAN.

Networking Requirements

A company has multiple services including the IPTV, VoIP, and Internet access services. Each service uses a unique protocol. It is required that services of the same type be transmitted in a VLAN and services of different types be transmitted in separate VLANs to facilitate management and reduce manual VLAN configuration workload.

As shown in **Figure 1-7**, the Switch receives packets of multiple services that use different protocols. Users in VLAN 10 use IPv4 to communicate with remote users, and users in VLAN 20 use IPv6 to communicate with the servers. The Switch needs to assign VLANs to packets of different services and transmit packets with different VLAN IDs to different servers.

Figure 1-7 Network diagram of protocol-based VLAN assignment



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and determine mappings between services and VLANs.
2. Associate protocols with VLANs.

   The Switch assigns a VLAN ID to a frame based on the protocol or protocol suite to which the frame belongs. As long as the protocols of user devices keep unchanged, users do not need to be added to new VLANs regardless of whether their locations change, whether network cards of PCs are changed, or whether users locate in the same network segment.
3. Configure a port to allow frames with specified VLAN IDs to pass through.
4. Associate ports with VLANs.

   After receiving a frame associated with a specified protocol, the system automatically assigns the VLAN ID associated with the protocol to the frame.

Data Preparation

To complete the configuration, you need the following data:

- VLANs to which XGE0/0/1 of the Switch needs to be added in untagged mode: VLAN 10 and VLAN 20
- VLANs to which XGE0/0/2 and XGE0/0/3 of the Switch need to be added in tagged mode: VLAN 10 and VLAN 20
- Protocol associated with each VLAN
  - VLAN 10: IPv4
  - VLAN 20: IPv6

Procedure

Step 1 Create VLANs.

Configure the Switch.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 10 20
```

Step 2 Configure protocol-based VLANs.

Associate IPv4 with VLAN 10.

```
[Switch] vlan 10
[Switch-vlan10] protocol-vlan ipv4
[Switch-vlan10] quit
```

Associate IPv6 with VLAN 20.

```
[Switch] vlan 20
[Switch-vlan20] protocol-vlan ipv6
[Switch-vlan20] quit
```

Step 3 Associate interfaces with protocol-based VLANs.

Associate XGE0/0/1 with VLAN 10 and set the 802.1p priority of VLAN 10 to 5.

```
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] protocol-vlan vlan 10 all priority 5
```

Associate XGE0/0/1 with VLAN 20 and set the 802.1p priority of VLAN 20 to 6.

```
[Switch-XGigabitEthernet0/0/1] protocol-vlan vlan 20 all priority 6
[Switch-XGigabitEthernet0/0/1] quit
```

Step 4 Configure interfaces.

Add XGE0/0/1 to VLAN 10 and VLAN 20 so that XGE0/0/1 allows packets of VLAN 10 and VLAN 20 to pass through.

```
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type hybrid
[Switch-XGigabitEthernet0/0/1] port hybrid untagged vlan 10 20
[Switch-XGigabitEthernet0/0/1] quit
```

Add XGE0/0/2 to VLAN 10 so that XGE0/0/2 allows packets of VLAN 10 to pass through.

```
[Switch] interface xgigabitethernet 0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Switch-XGigabitEthernet0/0/2] quit
```

Add XGE0/0/3 to VLAN 20 so that XGE0/0/3 allows packets of VLAN 20 to pass through.

```
[Switch] interface xgigabitethernet 0/0/3
[Switch-XGigabitEthernet0/0/3] port link-type trunk
[Switch-XGigabitEthernet0/0/3] port trunk allow-pass vlan 20
[Switch-XGigabitEthernet0/0/3] quit
```

Step 5 Verify the configuration.

After completing the configuration, run the **display protocol-vlan interface all** command, and you can view the configuration of protocol-based VLANs on XGE0/0/1. For example:

```
<Switch> display protocol-vlan interface all
--------------------------------------------------------------------------------
 Interface                VLAN    Index        Protocol Type           Priority
--------------------------------------------------------------------------------
 XGigabitEthernet0/0/1     10      0            ipv4                     5
 XGigabitEthernet0/0/1     20      0            ipv6                     6
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 10 20
#
vlan 10
 protocol-vlan 0 ipv4
vlan 20
 protocol-vlan 0 ipv6
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 10 20
 protocol-vlan vlan 10 0 priority 5
 protocol-vlan vlan 20 0 priority 6
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/3
 port link-type trunk
```

```
 port trunk allow-pass vlan 20
#
return
```

1.3.5 Example for Implementing Communication Between VLANs by Using VLANIF Interfaces

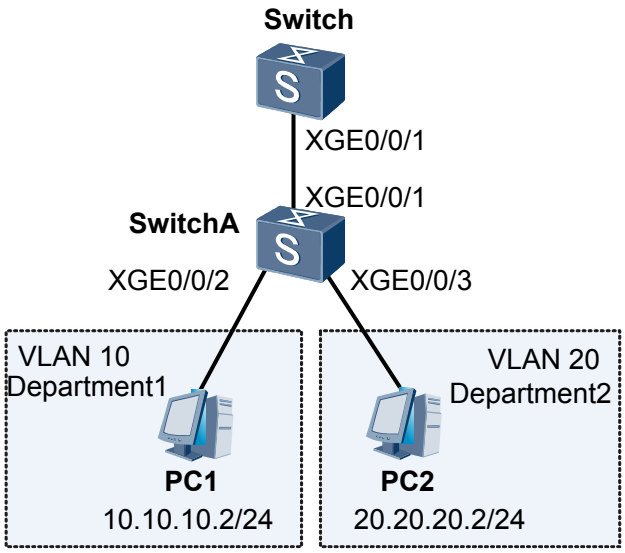
A Layer 3 switch can replace a router to implement communications between VLANs by using VLANIF interfaces.

Networking Requirements

Departments of an enterprise are located on different network segments and use same services such as Internet access and VoIP. Departments in different VLANs need to use the same service, so communication between VLANs must be implemented.

As shown in **Figure 1-8**, department 1 and department 2 use the same service but belong to different VLANs and are located on different network segments. Users in department 1 and department 2 need to communicate with each other.

Figure 1-8 Communication between VLANs using VLANIF interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the switches for different departments.
2. Add Layer 2 interfaces to the VLANs so that packets of the VLANs can pass through the Layer 2 interfaces.
3. On the Layer 3 switch, create VLANIF interfaces corresponding to the VLANs and configure IP addresses for the VLANIF interfaces to implement Layer 3 communication.

NOTE

To implement communication between VLANs, hosts in each VLAN must use the IP address of the corresponding VLANIF interface as gateway address.

Data Preparation

To complete the configuration, you need the following data:

- XGE0/0/1 of the Switch needs to be added to VLAN 10 and VLAN 20.
- The IP address of VLANIF10 on the Switch is 10.10.10.1/24.
- The IP address of VLANIF20 on the Switch is 20.20.20.1/24.
- XGE0/0/1of SwitchA needs to be added to VLAN 10 and VLAN 20.
- XGE0/0/2 of SwitchA needs to be added to VLAN 10.
- XGE0/0/3 of SwitchA needs to be added to VLAN 20.

Procedure

Step 1 # Configure the Switch.

Create VLANs.

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

Add XGE0/0/1 to VLANs.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type trunk
[Quidway-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
[Quidway-XGigabitEthernet0/0/1] quit
```

Assign IP addresses to VLANIF interfaces.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.10.10.1 24
[Quidway-Vlanif10] quit
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 20.20.20.1 24
[Quidway-Vlanif20] quit
```

Step 2 Configure SwitchA.

Create VLANs.

```
<Quidway> system-view
[Quidway] vlan batch 10 20
```

Add interfaces to VLANs.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type trunk
[Quidway-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 10
[Quidway-XGigabitEthernet0/0/2] quit
[Quidway] xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 20
[Quidway-XGigabitEthernet0/0/3] quit
```

Step 3 Verify the configuration.

On PC1 in VLAN 10, set the default gateway address to 10.10.10.1/24, which is the IP address of VLANIF10.

On PC2 in VLAN 20, set the default gateway address to 20.20.20.1/24, which is the IP address of VLANIF20.

After the preceding configurations are complete, PC1 in VLAN 10 and PC2 in VLAN 20 can communicate.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface Vlanif20
 ip address 20.20.20.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

Configuration file of SwitchA

```
#
 sysname Quidway
#
 vlan batch 10 20
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface XGigabitEthernet0/0/3
 port link-type access
 port default vlan 20
#
return
```

1.3.6 Example for Configuring VLAN Aggregation

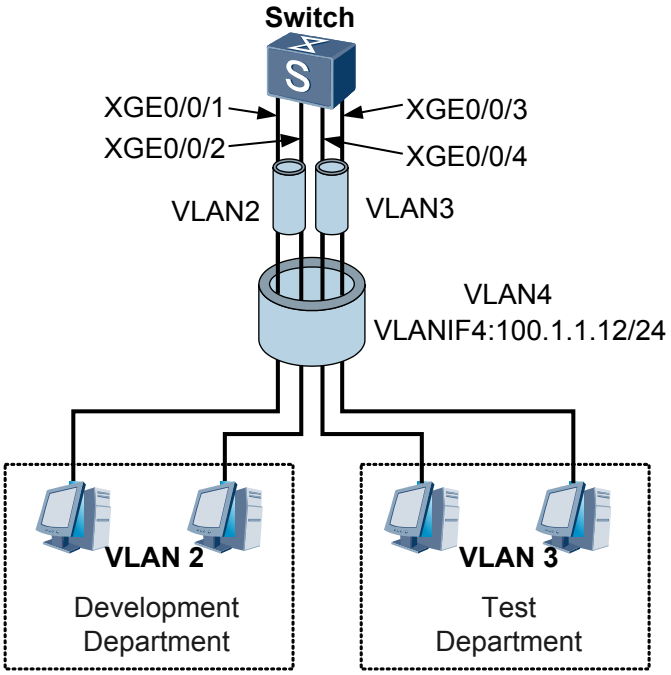
This part describes how to configure communication between VLANs with less IP addresses.

Networking Requirements

Assume that an enterprise has many departments and IP addresses of these departments are on the same network segment, to improve the service security, IP address of employee users in different departments are added to different VLANs. Employee users in different departments need to communicate with each other.

As shown in **Figure 1-9**, IP addresses of the R&D department and test department belong to different VLANs. It is required that employee users in different VLANs communicate with each other.

Figure 1-9 Typical networking of VLAN configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Add interfaces of the Switch to sub-VLANs.
2. Add the sub-VLANs to a super-VLAN.
3. Configure the IP address for the super-VLAN.
4. Configure proxy ARP for the super-VLAN.

Data Preparation

To complete the configuration, you need the following data:

- XGE 0/0/1 and XGE 0/0/2 belong to VLAN 2.
- XGE 0/0/3 and XGE 0/0/4 belong to VLAN 3.
- The VLAN ID of the super-VLAN is 4.
- The IP address of the super-VLAN is 100.1.1.12.

Procedure

Step 1 Set the interface type.

Configure XGE 0/0/1 as an access interface.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
[Quidway-XGigabitEthernet0/0/1] quit
```

Configure XGE 0/0/2 as an access interface.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure XGE 0/0/3 as an access interface.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] port link-type access
[Quidway-XGigabitEthernet0/0/3] quit
```

Configure XGE 0/0/4 as an access interface.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/4
[Quidway-XGigabitEthernet0/0/4] port link-type access
[Quidway-XGigabitEthernet0/0/4] quit
```

Step 2 Configure VLAN 2.

Create VLAN 2.

```
[Quidway] vlan 2
```

Add XGE 0/0/1 and XGE 0/0/2 to VLAN 2.

```
[Quidway-vlan2] port xgigabitethernet 0/0/1 0/0/2
[Quidway-vlan2] quit
```

Step 3 Configure VLAN 3.

Create VLAN 3.

```
[Quidway] vlan 3
```

Add XGE 0/0/3 and XGE 0/0/4 to VLAN 3.

```
[Quidway-vlan3] port xgigabitethernet 0/0/3 0/0/4
[Quidway-vlan3] quit
```

Step 4 Configure VLAN 4.

Configure the super-VLAN.

```
[Quidway] vlan 4
[Quidway-vlan4] aggregate-vlan
[Quidway-vlan4] access-vlan 2 to 3
```

Configure the VLANIF interface.

```
[Quidway] interface vlanif 4
[Quidway-Vlanif4] ip address 100.1.1.12 255.255.255.0
[Quidway-Vlanif4] quit
```

Step 5 Configure the personal computers.

Configure the IP address for each personal computer and make them reside in the same network segment with VLAN 4.

After the preceding configuration, the personal computers and the Switch can ping each other, but the computers in VLAN 2 and the computers in VLAN 3 cannot ping each other.

Step 6 Configure proxy ARP.

```
[Quidway] interface vlanif 4
[Quidway-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
```

Step 7 Verify the configuration.

After the preceding configuration, the computers in VLAN 2 and the computers in VLAN 3 can ping each other.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
#
interface Vlanif4
 ip address 100.1.1.12 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface XGigabitEthernet0/0/3
 port link-type access
 port default vlan 3
#
interface XGigabitEthernet0/0/4
 port link-type access
 port default vlan 3
#
return
```

1.3.7 Example for Configuring the MUX VLAN

MUX VLAN isolates Layer 2 traffic of different interfaces in a VLAN. It allows some employee users of an enterprise to communicate with each other and isolates some employee users from each other.

Networking Requirements

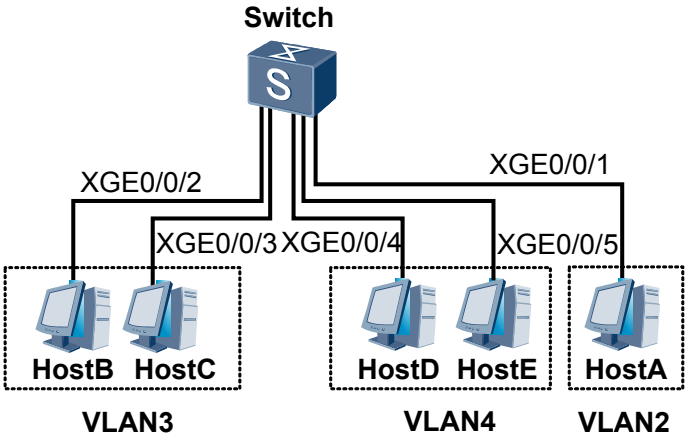
In an enterprise network, all employees of the enterprise can access the enterprise's server. It is required that some employees be able to communicate with each other, whereas some employees not communicate with each other.

As shown in **Figure 1-10**, in an enterprise network, all employees of the enterprise can access the enterprise's server. It is required that some employees be able to communicate with each other, whereas some employees not communicate with each other.

For an enterprise with a large number of employees, each employee that is prohibited from communicating with another needs to be added to a separate VLAN if the preceding scheme is used. This wastes VLAN ID resources and imposes an additional configuration workload on the network administrator.

Configuring a MUX VLAN on the switch connected to PCs helps to save VLAN ID resources, reduce the configuration workload of the network administrator, and facilitate network maintenance.

Figure 1-10 Typical networking of MUX VLAN configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the MUX VLAN.
2. Configure the group VLAN.
3. Configure the separate VLAN.
4. Add interfaces to the VLAN and enable the MUX VLAN function.

Data Preparation

To complete the configuration, you need the following data:

- XGE 0/0/1 belongs to VLAN 2.
- XGE 0/0/2 and XGE 0/0/3 belong to VLAN 3.
- XGE 0/0/4 and XGE 0/0/5 belong to VLAN 4.

Procedure

Step 1 Configure the MUX VLAN.

Create VLAN 2, VLAN 3, and VLAN 4.

```
<Quidway> system-view
[Quidway] vlan batch 2 3 4
[Quidway] quit
```

Configure the MUX VLAN, subordinate VLAN, and interfaces.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] mux-vlan
[Quidway-vlan2] subordinate group 3
```

```
[Quidway-vlan2] subordinate separate 4
[Quidway-vlan2] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
[Quidway-XGigabitEthernet0/0/1] port default vlan 2
[Quidway-XGigabitEthernet0/0/1] port mux-vlan enable
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 3
[Quidway-XGigabitEthernet0/0/2] port mux-vlan enable
[Quidway-XGigabitEthernet0/0/2] quit
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] port link-type access
[Quidway-XGigabitEthernet0/0/3] port default vlan 3
[Quidway-XGigabitEthernet0/0/3] port mux-vlan enable
[Quidway-XGigabitEthernet0/0/3] quit
[Quidway] interface xgigabitethernet 0/0/4
[Quidway-XGigabitEthernet0/0/4] port link-type access
[Quidway-XGigabitEthernet0/0/4] port default vlan 4
[Quidway-XGigabitEthernet0/0/4] port mux-vlan enable
[Quidway-XGigabitEthernet0/0/4] quit
[Quidway] interface xgigabitethernet 0/0/5
[Quidway-XGigabitEthernet0/0/5] port link-type access
[Quidway-XGigabitEthernet0/0/5] port default vlan 4
[Quidway-XGigabitEthernet0/0/5] port mux-vlan enable
[Quidway-XGigabitEthernet0/0/5] quit
```

Step 2 Verify the configuration.

Host A can ping Hosts B to E. Hosts B to E can also ping Host A.

Host B and Host C can ping each other.

Host D and Host E cannot ping each other.

Host B and Host C cannot ping Host D or host E. Host D and Host E cannot ping Host B or Host C.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate group 3
 subordinate separate 4
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 2
 port mux-vlan enable
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 3
 port mux-vlan enable
#
interface XGigabitEthernet0/0/3
 port link-type access
```

```
 port default vlan 3
 port mux-vlan enable
#
interface XGigabitEthernet0/0/4
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
interface XGigabitEthernet0/0/5
 port link-type access
 port default vlan 4
 port mux-vlan enable
#
return
```

1.3.8 Example for Configuring a Voice VLAN in Auto Mode

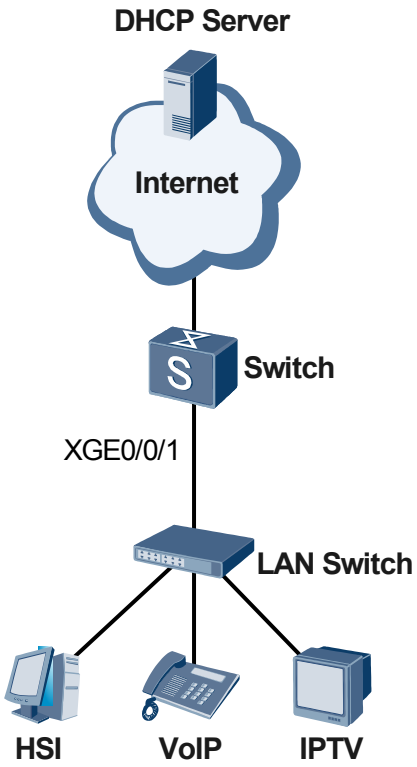
In this example, voice traffic is transmitted by using a specific VLAN, namely, voice VLAN. During a certain period, if a voice device becomes faulty or exits from the network, the interface connected to the voice device will exit from the voice VLAN.

Networking Requirements

Data flows of the HSI, VoIP, and IPTV services are transmitted on a network. Users require high quality of VoIP services; therefore, voice data flows must be transmitted with a high priority to ensure the call quality.

As shown in **Figure 1-11**, after a voice VLAN is configured on the Switch, the Switch checks whether a data flow received by XGigabitEthernet0/0/1 is a voice data flow based on the source MAC address of the flow. If the data flow is a voice data flow, the Switch changes the priority of the flow and transmits it in the voice VLAN. If not, the Switch transmits the flow in a common VLAN without changing the priority of the flow. XGigabitEthernet0/0/1 needs to be automatically added to or deleted from the voice VLAN.

Figure 1-11 Networking diagram of configuring a voice VLAN in auto mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs.
2. Configure the link type and default VLAN of the interface.
3. Enable the voice VLAN on the interface.
4. Set the mode of adding the interface to the voice VLAN to auto.
5. Set the OUI of the voice VLAN.
6. Set the aging time of the voice VLAN.
7. Set the working mode of the voice VLAN.

Data Preparation

To complete the configuration, you need the following data:

- Voice VLAN and VLAN through which the IP phone applies for an IP address: VLAN 2 and VLAN 6
- OUI and mask: 0011-2200-0000 and ffff-ff00-0000
- Aging time of the voice VLAN: 100 minutes
- The default VLAN of XGigabitEthernet 0/0/1 is VLAN 6.

Procedure

Step 1 Create VLANs and configure the interface on the Switch.

Create VLAN 2 and VLAN 6.

```
<Quidway> system-view
[Quidway] vlan batch 2 6
```

Configure the link type and default VLAN of the interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 6
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 6
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Configure the voice VLAN on the Switch.

Configure the voice VLAN on the interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] voice-vlan 2 enable
```

Set the mode of adding the interface to the voice VLAN to auto.

```
[Quidway-XGigabitEthernet0/0/1] voice-vlan mode auto
[Quidway-XGigabitEthernet0/0/1] quit
```

Set the OUI of the voice VLAN.

```
[Quidway] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

Set the aging time of the voice VLAN.

```
[Quidway] voice-vlan aging-time 100
```

Set the working mode of the voice VLAN.

```
[Quidway-XGigabitEthernet0/0/1] voice-vlan security enable
```

Step 3 Verify the configuration.

Run the **display voice-vlan oui** command to check whether the OUI of the voice VLAN is correct.

```
<Quidway> display voice-vlan oui
-------------------------------------------------
OuiAddress       Mask             Description
-------------------------------------------------
0011-2200-0000   ffff-ff00-0000
```

Run the **display voice-vlan 2 status** command to check whether the mode of adding the interface to the voice VLAN, working mode, and aging time of the voice VLAN are correct.

```
<Quidway> display voice-vlan 2 status
Voice VLAN Configurations:
-------------------------------------------------
Voice VLAN ID            :  2
Voice VLAN status        : Enable
Voice VLAN aging time    : 100 (minutes)
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
-------------------------------------------------------------
Port Information:
-------------------------------------------------------------
Port                     Add-Mode  Security-Mode  Legacy
```

```
-------------------------------------------------------------
XGigabitEthernet0/0/1     Auto      Security       Disable
```

----End

Configuration Files

Configuration file of the Switch

```
#
sysname Quidway
#
 vlan batch 2 6
#
 voice-vlan aging-time 100
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 6
 port hybrid untagged vlan 6
 voice-vlan 2 enable
#
return
```

1.3.9 Example for Configuring a Voice VLAN in Manual Mode

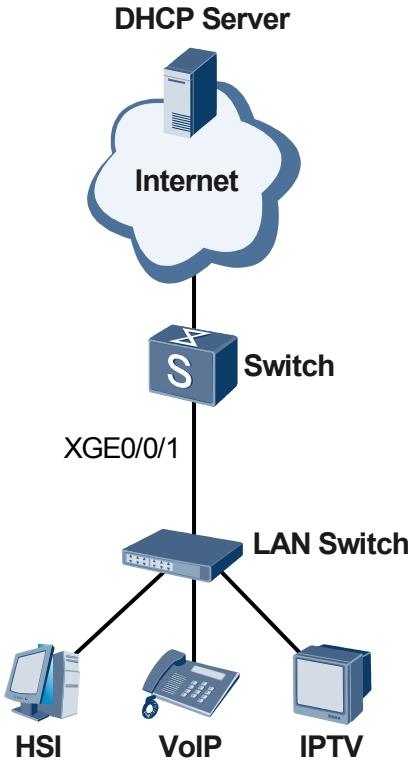
In manual voice VLAN mode, an interface must be added to the voice VLAN manually after the voice VLAN function is enabled on the interface. The interface connected to a voice device can forward voice data packets only after the interface is added to the voice VLAN manually.

Networking Requirements

Data flows of the HSI, VoIP, and IPTV services are transmitted on a network. Users require high quality of VoIP services; therefore, voice data flows must be transmitted with a high priority to ensure the call quality.

As shown in **Figure 1-12**, after a voice VLAN is configured on the Switch, the Switch checks whether a data flow received by XGigabitEthernet0/0/1 is a voice data flow based on the source MAC address of the flow. If the data flow is a voice data flow, the Switch changes the priority of the flow and transmits it in the voice VLAN. If not, the Switch transmits the flow in a common VLAN without changing the priority of the flow. XGigabitEthernet0/0/1 needs to be added to or deleted from the voice VLAN manually.

Figure 1-12 Networking diagram of a voice VLAN in manual mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs.
2. Configure the link type and default VLAN of the interface.
3. Enable the voice VLAN on the interface.
4. Set the mode of adding the interface to the voice VLAN to manual.
5. Set the OUI of the voice VLAN.
6. Set the working mode of the voice VLAN.
7. Add the interface to the voice VLAN.

Data Preparation

To complete the configuration, you need the following data:

- Voice VLAN and VLAN through which the IP phone applies for an IP address: VLAN 2 and VLAN 6
- OUI and mask: 0011-2200-0000 and ffff-ff00-0000
- Default VLAN of XGigabitEthernet 0/0/1: VLAN 6

Procedure

Step 1 Create VLANs and configure the interface on the Switch.

Create VLAN 2 and VLAN 6.

```
<Quidway> system-view
[Quidway] vlan batch 2 6
```

Configure the link type and default VLAN of the interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 6
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 6
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Configure the voice VLAN on the Switch.

Configure the voice VLAN on the interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] voice-vlan 2 enable
```

Set the mode of adding the interface to the voice VLAN to manual and add the interface to the voice VLAN.

```
[Quidway-XGigabitEthernet0/0/1] voice-vlan mode manual
[Quidway-XGigabitEthernet0/0/1] port hybrid tagged vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
```

Set the OUI of the voice VLAN.

```
[Quidway] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
```

Set the working mode of the voice VLAN.

```
[Quidway-XGigabitEthernet0/0/1] voice-vlan security enable
```

Step 3 Verify the configuration.

Run the **display voice-vlan oui** command to check whether the OUI of the voice VLAN is correct.

```
<Quidway> display voice-vlan oui
-------------------------------------------------
OuiAddress       Mask             Description
-------------------------------------------------
0011-2200-0000   ffff-ff00-0000
```

Run the **display voice-vlan 2 status** command to check whether the mode of adding the interface to the voice VLAN, working mode, and aging time of the voice VLAN are correct.

```
<Quidway> display voice-vlan 2 status
Voice VLAN Configurations:
-------------------------------------------------
Voice VLAN ID            :  2
Voice VLAN status        : Enable
Voice VLAN aging time    : 1440 (minutes)
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
-------------------------------------------------------------
Port Information:
-------------------------------------------------------------
Port                     Add-Mode  Security-Mode  Legacy
-------------------------------------------------------------
XGigabitEthernet0/0/1     Manual    Security       Disable
```

----End

Configuration Files

Configuration file of the Switch

```
#
sysname Quidway
#
 vlan batch 2 6
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 6
 port hybrid tagged vlan 2
 port hybrid untagged vlan 6
 voice-vlan 2 enable
 voice-vlan mode manual
#
return
```

1.4 VLAN Mapping Configuration

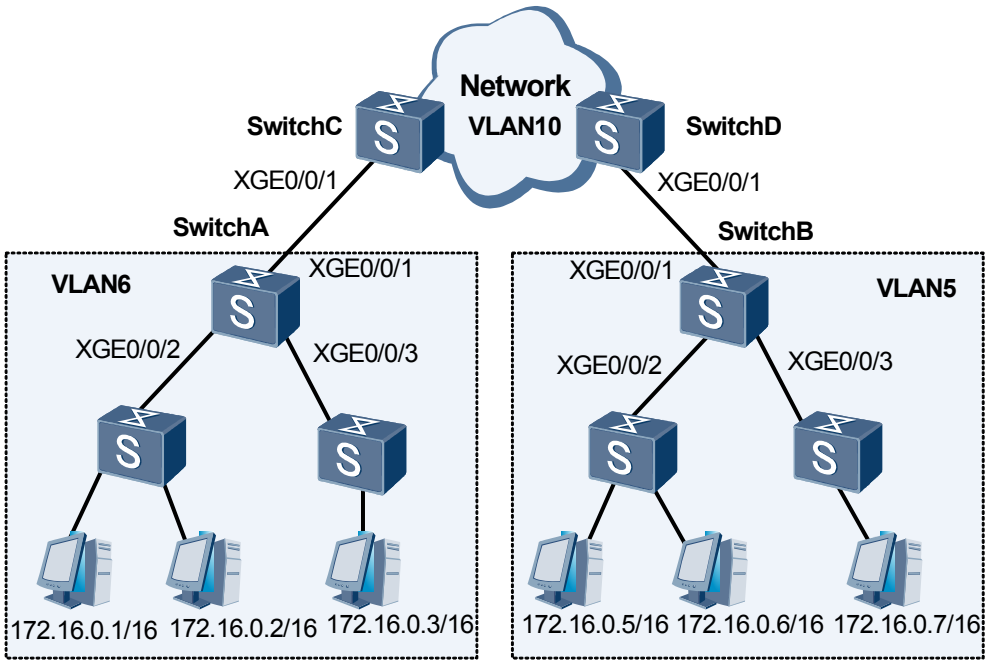
This chapter describes the basic knowledge, methods, and examples for configuring VLAN mapping.

1.4.1 Example for Configuring Single-Tag VLAN Mapping

Networking Requirements

As shown in **Figure 1-13**, users in VLAN 6 need to communicate with users in VLAN 5 through VLAN 10 on the network.

Figure 1-13 Networking diagram of single-tag VLAN mapping configurations



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on SwitchA, SwitchB, SwitchC, and SwitchD.
2. Add interfaces of SwitchA, SwitchB, SwitchC, and SwitchD to the corresponding VLANs.
3. Configure single-tag VLAN mapping on XGE 0/0/1 of SwitchA.
4. Configure single-tag VLAN mapping on XGE 0/0/1 of SwitchB.

Data Preparation

To complete the configuration, you need the following data:

- VLAN to be created on SwitchA: VLAN 6
- VLAN to be created on SwitchB: VLAN 5
- VLAN to be created on SwitchC and SwitchD: VLAN 10

Procedure

Step 1 Create VLANs on the Switches.

Create VLAN 6 on SwitchA.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 6
```

Create VLAN 5 on SwitchB.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 5
```

Create VLAN 10 on SwitchC.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan 10
```

Create VLAN 10 on SwitchD.

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] vlan 10
```

Step 2 Add interfaces to VLANs.

Add XGE 0/0/2 and XGE 0/0/3 of SwitchA to VLAN 6.

```
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 6
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] port link-type trunk
[SwitchA-XGigabitEthernet0/0/3] port trunk allow-pass vlan 6
[SwitchA-XGigabitEthernet0/0/3] quit
```

Add XGE 0/0/1 of SwitchA to VLAN 6.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
```

```
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 6
[SwitchA-XGigabitEthernet0/0/1] quit
```

Add XGE 0/0/2 and XGE 0/0/3 of SwitchB to VLAN 5.

```
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] port link-type trunk
[SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 5
[SwitchB-XGigabitEthernet0/0/2] quit
[SwitchB] interface xgigabitethernet 0/0/3
[SwitchB-XGigabitEthernet0/0/3] port link-type trunk
[SwitchB-XGigabitEthernet0/0/3] port trunk allow-pass vlan 5
[SwitchB-XGigabitEthernet0/0/3] quit
```

Add XGE 0/0/1 of SwitchB to VLAN 5.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 5
[SwitchB-XGigabitEthernet0/0/1] quit
```

Add XGE 0/0/1 of SwitchC to VLAN 10.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port link-type trunk
[SwitchC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchC-XGigabitEthernet0/0/1] quit
```

Add XGE 0/0/1 of SwitchD to VLAN 10.

```
[SwitchD] interface xgigabitethernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] port link-type trunk
[SwitchD-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchD-XGigabitEthernet0/0/1] quit
```

Step 3 Configure single-tag VLAN mapping on the Switches.

Configure single-tag VLAN mapping on XGE 0/0/1 of SwitchA.

```
[SwitchA-XGigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchA-XGigabitEthernet0/0/1] port vlan-mapping vlan 10 map-vlan 6
```

Configure single-tag VLAN mapping on XGE 0/0/1 of SwitchB.

```
[SwitchB-XGigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchB-XGigabitEthernet0/0/1] port vlan-mapping vlan 10 map-vlan 5
```

Step 4 Verify the configuration.

The hosts in VLAN 6 and the hosts in VLAN 5 can ping each other.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
vlan batch 6
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port link-type trunk
 port trunk allow-pass vlan 6
 port vlan-mapping vlan 10 map-vlan 6
#
interface XGigabitEthernet0/0/2
```

```
 port link-type trunk
 port trunk allow-pass vlan 6
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 6
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
vlan batch 5
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port link-type trunk
 port trunk allow-pass vlan 5
 port vlan-mapping vlan 10 map-vlan 5
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 5
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

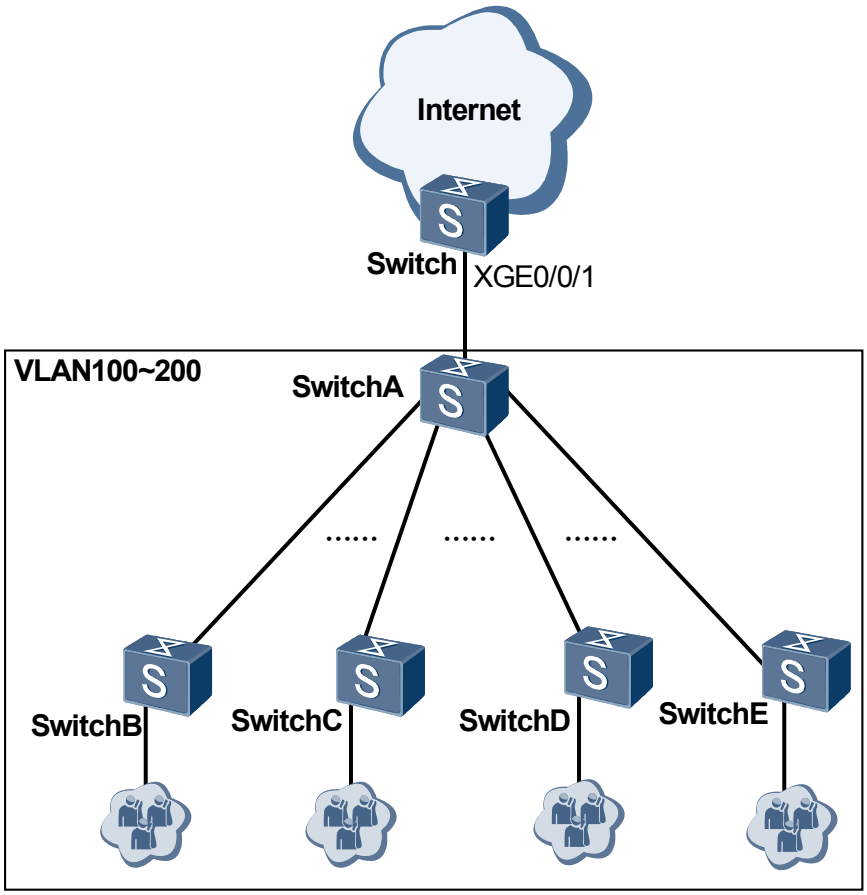
1.4.2 Example for Configuring N:1 VLAN Mapping

Networking Requirements

As shown in **Figure 1-14**, users in VLAN 100 to VLAN 200 connect to the Internet through the aggregate switch of the carrier, that is, the Switch.

After user devices are powered on, they send service request packets to the switch of the carrier. After the user devices pass the authentication, services can be used.

Figure 1-14 Networking diagram for configuring N:1 VLAN mapping



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the VLANs before and after mapping.
2. Add XGE 0/0/1 of the Switch to the VLANs before and after mapping in tagged mode.
3. Configure VLAN mapping on XGE 0/0/1 of the Switch.

Data preparation

To complete the configuration, you need the following data:

- VLANs before mapping: VLAN 100 to VLAN 200
- VLAN after mapping: VLAN 10

Procedure

Step 1 Configure the Switch.

Create VLANs.

```
<Quidway> system-view
[Quidway] vlan batch 10 100 to 200
```

Add related XGE 0/0/1 to the VLANs.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid tagged vlan 10 100 to 200
```

Configure VLAN mapping on XGE 0/0/1.

```
[Quidway-XGigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-XGigabitEthernet0/0/1] port vlan-mapping vlan 100 to 200 map-vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Verify the configuration.

Users in VLAN 100 to VLAN 200 can connect to the Internet through the Switch.

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Quidway
#
vlan batch 10 100 to 200
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid tagged vlan 10 100 to 200
 port vlan-mapping vlan 100 to 200 map-vlan 10
#
return
```

1.5 QinQ Configuration

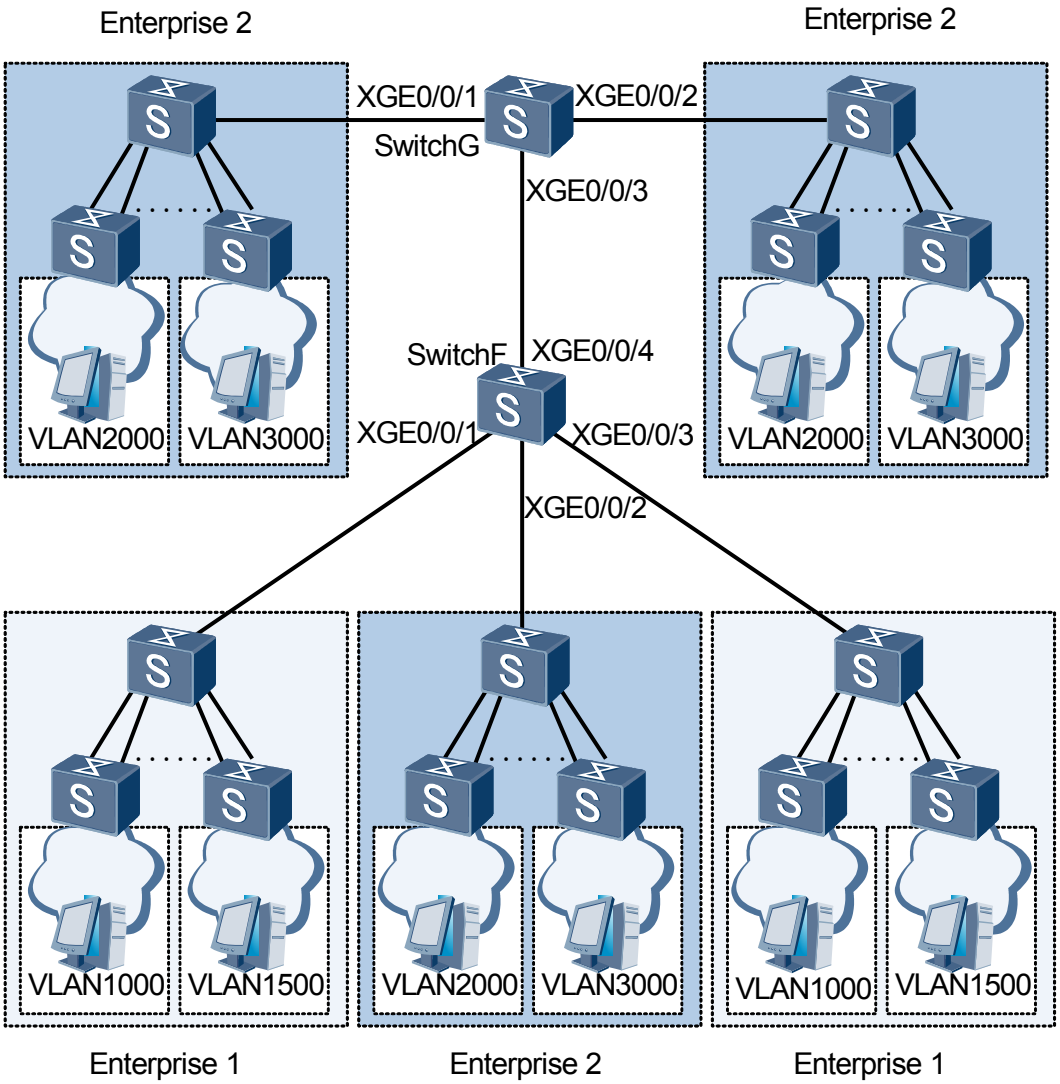
This chapter describes the basic knowledge, methods, and examples for configuring QinQ.

1.5.1 Example for Configuring QinQ on Interfaces

Networking Requirements

As shown in **Figure 1-15**, there are two enterprises on the network, namely, Enterprise 1 and Enterprise 2. Enterprise 1 has two office locations; Enterprise 2 has three office locations. The office locations of the two enterprises access SwitchG or SwitchF of the ISP network. The network of Enterprise 1 is divided into VLAN 1000 to VLAN 1500; the network of Enterprise 2 is divided into VLAN 2000 to VLAN 3000. It is required that employees in the same VLAN can communicate with each other through the ISP network but the two enterprises are isolated from each other.

Figure 1-15 Networking diagram for configuring QinQ on interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 10 and VLAN 20 on SwitchF; create VLAN 20 on SwitchG.
2. Configure XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 of SwitchF as QinQ interfaces.
3. Configure XGE 0/0/1 and XGE 0/0/2 of SwitchG as QinQ interfaces.
4. Add XGE 0/0/4 of SwitchF and XGE 0/0/3 of SwitchG to VLAN 20 in tagged mode.

Data Preparation

To complete the configuration, you need the following data:

- VLAN 10 assigned to Enterprise 1 on the ISP network
- VLAN 20 assigned to Enterprise 2 on the ISP network.

Procedure

Step 1 Create VLANs.

Create VLAN 10 and VLAN 20 on SwitchF.

```
<Quidway> system-view
[Quidway] sysname SwitchF
[SwitchF] vlan batch 10 20
```

Create VLAN 20 on SwitchG.

```
<Quidway> system-view
[Quidway] sysname SwitchG
[SwitchG] vlan 20
```

Step 2 Configure the interfaces as QinQ interfaces.

Configure XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 of SwitchF as QinQ interfaces. Set the VLAN ID of the outer VLAN tag added by XGE 0/0/1 and XGE 0/0/3/ to VLAN 10; set the VLAN ID of the outer VLAN tag added by XGE 0/0/2 to VLAN 20.

```
[SwitchF] interface xgigabitethernet 0/0/1
[SwitchF-XGigabitEthernet0/0/1] port link-type dot1q-tunnel
[SwitchF-XGigabitEthernet0/0/1] port default vlan 10
[SwitchF-XGigabitEthernet0/0/1] quit
[SwitchF] interface xgigabitethernet 0/0/2
[SwitchF-XGigabitEthernet0/0/2] port link-type dot1q-tunnel
[SwitchF-XGigabitEthernet0/0/2] port default vlan 20
[SwitchF-XGigabitEthernet0/0/2] quit
[SwitchF] interface xgigabitethernet 0/0/3
[SwitchF-XGigabitEthernet0/0/3] port link-type dot1q-tunnel
[SwitchF-XGigabitEthernet0/0/3] port default vlan 10
[SwitchF-XGigabitEthernet0/0/3] quit
```

Set XGE 0/0/1 and XGE 0/0/2 of SwitchG as QinQ interfaces; set the VLAN ID of the outer VLAN tags added by XGE 0/0/1 and XGE 0/0/2/ to VLAN 20.

```
[SwitchG] interface xgigabitethernet 0/0/1
[SwitchG-XGigabitEthernet0/0/1] port link-type dot1q-tunnel
[SwitchG-XGigabitEthernet0/0/1] port default vlan 20
[SwitchG-XGigabitEthernet0/0/1] quit
[SwitchG] interface xgigabitethernet 0/0/2
[SwitchG-XGigabitEthernet0/0/2] port link-type dot1q-tunnel
[SwitchG-XGigabitEthernet0/0/2] port default vlan 20
[SwitchG-XGigabitEthernet0/0/2] quit
```

Step 3 Configure other interfaces.

Add XGE 0/0/4 of SwitchF to VLAN 20.

```
[SwitchF] interface xgigabitethernet 0/0/4
[SwitchF-XGigabitEthernet0/0/4] port link-type trunk
[SwitchF-XGigabitEthernet0/0/4] port trunk allow-pass vlan 20
[SwitchF-XGigabitEthernet0/0/4] quit
```

Add XGE 0/0/3 of SwitchG to VLAN 20.

```
[SwitchG] interface xgigabitethernet 0/0/3
[SwitchG-XGigabitEthernet0/0/3] port link-type trunk
[SwitchG-XGigabitEthernet0/0/3] port trunk allow-pass vlan 20
[SwitchG-XGigabitEthernet0/0/3] quit
```

Step 4 Verify the configuration.

Ping a remote host on the same VLAN in another office location of Enterprise 1 from a host of Enterprise 1. If it can ping the remote host, hosts in different locations of Enterprise 1 can communicate with each other.

Ping a remote host on the same VLAN in another office location of Enterprise 2 from a host of Enterprise 2. If it can ping the remote host, hosts in different locations of Enterprise 2 can communicate with each other.

Ping a host of Enterprise 2 from a host in any office location of Enterprise 1. If it fails to ping the host of Enterprise 2, the two enterprises are isolated from each other.

----End

Configuration Files

The following lists the configuration files of the Switch.

- Configuration file of SwitchF

```
#
 sysname SwitchF
#
 vlan batch 10 20
#
interface XGigabitEthernet0/0/1
 port link-type dot1q-tunnel
 port default vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type dot1q-tunnel
 port default vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type dot1q-tunnel
 port default vlan 10
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

- Configuration file of SwitchG

```
#
 sysname SwitchG
#
 vlan batch 20
#
interface XGigabitEthernet0/0/1
 port link-type dot1q-tunnel
 port default vlan 20
#
interface XGigabitEthernet0/0/2
 port link-type dot1q-tunnel
 port default vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

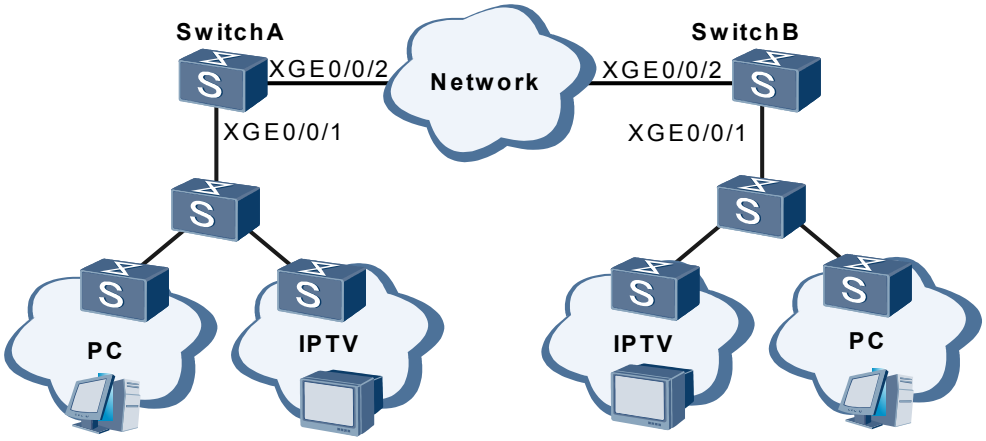
1.5.2 Example for Configuring Selective QinQ

Networking Requirements

As shown in **Figure 1-16**, common Internet access users (using PCs) and IPTV users (using IPTV terminals) connect to the carrier network through Switch A and Switch B and communicate with each other through the carrier network.

It is required that packets of PCs and IPTV terminals are tagged VLAN 2 and VLAN 3 when the packets are transmitted through the carrier network.

Figure 1-16 Networking for configuring selective QinQ



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on Switch A and Switch B.
2. Configure types of interfaces on Switch A and Switch B, and add the interfaces to corresponding VLANs.
3. Configure selective QinQ on interfaces of Switch A and Switch B.

Data Preparation

To complete the configuration, you need the following data:

- VLANs that PCs belong to: VLAN 100 to VLAN 200
- VLANs that IPTV terminals belong to: VLAN 300 to VLAN 400
- VLAN tag that packets of PCs carry on the carrier network: VLAN 2
- VLAN tag that packets of IPTV terminals carry on the carrier network: VLAN 3

Procedure

Step 1 Create VLANs.

On Switch A, create VLAN 2 and VLAN 3, that is, the outer VLAN IDs added to packets on the carrier network.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 2 3
```

On Switch B, create VLAN 2 and VLAN 3, that is, the outer VLAN IDs added to packets on the carrier network.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 2 3
```

Step 2 Configure selective QinQ on interfaces of Switch A and Switch B.

Configure XGE 0/0/1 of Switch A.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type hybrid
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 2 3
[SwitchA-XGigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchA-XGigabitEthernet0/0/1] port vlan-stacking vlan 100 to 200 stack-vlan 2
[SwitchA-XGigabitEthernet0/0/1] port vlan-stacking vlan 300 to 400 stack-vlan 3
[SwitchA-XGigabitEthernet0/0/1] quit
```

Configure XGE 0/0/1 of Switch B.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type hybrid
[SwitchB-XGigabitEthernet0/0/1] port hybrid untagged vlan 2 3
[SwitchB-XGigabitEthernet0/0/1] qinq vlan-translation enable
[SwitchB-XGigabitEthernet0/0/1] port vlan-stacking vlan 100 to 200 stack-vlan 2
[SwitchB-XGigabitEthernet0/0/1] port vlan-stacking vlan 300 to 400 stack-vlan 3
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 3 Configure other interfaces.

Add XGE 0/0/2 of Switch A to VLAN 2 and VLAN 3.

```
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 3
[SwitchA-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/2 of Switch B to VLAN 2 and VLAN 3.

```
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] port link-type trunk
[SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 3
[SwitchB-XGigabitEthernet0/0/2] quit
```

Step 4 Verify the configuration.

View the configuration of each interface on Switch A.

```
<SwitchA> display current-configuration interface xgigabitethernet 0/0/1
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
return
<SwitchA> display current-configuration interface xgigabitethernet 0/0/2
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

View the configuration of each interface on Switch B.

```
<SwitchB> display current-configuration interface xgigabitethernet 0/0/1
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
return
<SwitchB> display current-configuration interface xgigabitethernet 0/0/2
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

If Switch A and Switch B are configured correctly:

- PCs can communicate with each other through the carrier network.
- IPTV terminals can communicate with each other through the carrier network.

----End

Configuration Files

Only the configuration files of the Switches are provided:

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 2 to 3
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 2 to 3
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid untagged vlan 2 to 3
 port vlan-stacking vlan 100 to 200 stack-vlan 2
 port vlan-stacking vlan 300 to 400 stack-vlan 3
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

1.5.3 Example for Configuring Selective QinQ with VLAN Mapping

Networking Requirements

As shown in **Figure 1-17**, the Internet access, IPTV, and VoIP services are provided for users through home gateways.

The corridor switches allocate VLANs to the services as follows:

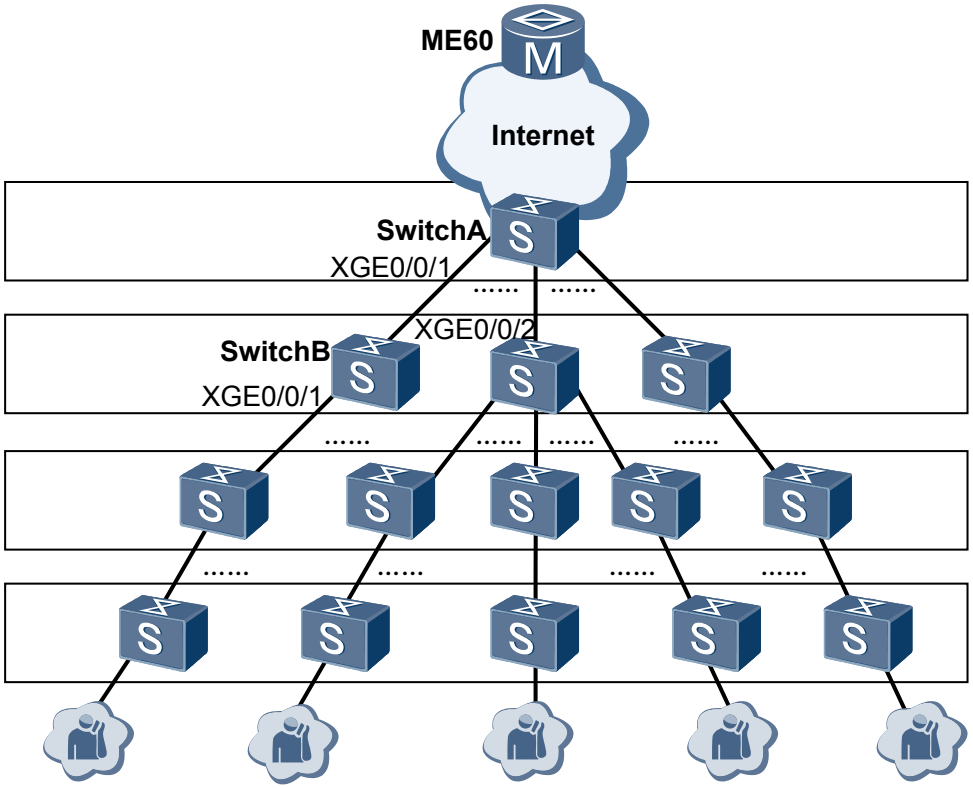
- VLANs for the Internet access service of different users: VLAN 1000 to VLAN 1100
- Shared VLAN for the IPTV service: VLAN 1101
- Shared VLAN for the VoIP service: VLAN 1102
- Shared VLAN for home gateways: VLAN 1103

Each community switch is connected to 50 downstream corridor switches and maps the VLAN IDs in the packets of the Internet access service from the corridor switches to VLAN 101 to VLAN 150.

The aggregate switch of the carrier is connected to 50 downstream community switches and adds outer VLAN IDs 21 to 70 to the packets sent from the community switches.

After user devices are powered on, they send service request packets to the switch of the carrier. After the user devices pass the authentication, services can be used.

Figure 1-17 Networking for configuring selective QinQ



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on SwitchA and SwitchB.
2. Configure VLAN mapping on SwitchB and add XGE 0/0/1 and XGE 0/0/2 to the VLANs.
3. Configure selective QinQ on SwitchA and add XGE 0/0/1 to VLANs.
4. Add other downlink interfaces of SwitchA and SwitchB to the VLANs. The configurations are similar to the configurations of their XGE 0/0/1 interfaces.
5. Configure other community switches. The configuration is similar to the configuration on SwitchB.

Data preparation

To complete the configuration, you need the following data:

- VLANs to which XGE 0/0/1 of SwitchB is added in tagged mode: VLAN 1000 to VLAN 1100, VLAN 1101, VLAN 1102, VLAN 1103, and VLAN 101
- VLANs to which XGE 0/0/2 of SwitchB is added in tagged mode: VLAN 101 to VLAN 150, VLAN 1101, VLAN 1102, and VLAN 1103
- VLANs to which XGE 0/0/1 of SwitchA is added in tagged mode: VLAN 1101, VLAN 1102, and VLAN 1103
- VLANs to which XGE 0/0/1 of SwitchA is added in untagged mode: VLAN 21
- Interface on SwitchB where VLAN mapping is configured: XGE 0/0/1
- Interface on SwitchA where selective QinQ is configured: XGE 0/0/1

Procedure

Step 1 # Configure SwitchA.

Create VLANs.

```
<Quidway> system-view
[Quidway] vlan batch 21 to 70 1101 to 1103
```

Add related XGE 0/0/1 to the VLANs.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 21
[Quidway-XGigabitEthernet0/0/1] port hybrid tagged vlan 1101 to 1103
[Quidway-XGigabitEthernet0/0/1] quit
```

Configure selective QinQ on XGE 0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-XGigabitEthernet0/0/1] port vlan-stacking vlan 101 to 150 stack-vlan 21
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 # Configure SwitchB.

Create VLANs.

```
<Quidway> system-view
[Quidway] vlan batch 101 to 150 1000 to 1103
```

Add XGE 0/0/1 and XGE 0/0/2 to the VLANs.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid tagged vlan 101 1000 to 1103
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid tagged vlan 101 to 150 1101 to 1103
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure VLAN mapping on XGE 0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] qinq vlan-translation enable
[Quidway-XGigabitEthernet0/0/1] port vlan-mapping vlan 1000 to 1100 map-vlan 101
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 3 Verify the configuration.

The Internet access service, IPTV service, and VoIP service can be used.

----End

Configuration Files

Configuration file of SwitchA

```
#
 sysname Quidway
#
 vlan batch 21 to 70 1101 to 1103
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid tagged vlan 1101 to 1103
 port hybrid untagged vlan 21
 port vlan-stacking vlan 101 to 150 stack-vlan 21
#
return
```

Configuration file of SwitchB

```
#
 sysname Quidway
#
 vlan batch 101 to 150 1000 to 1103
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid tagged vlan 101 1000 to 1103
 port vlan-mapping vlan 1000 to 1100 map-vlan 101
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 101 to 150 1101 to 1103
#
return
```

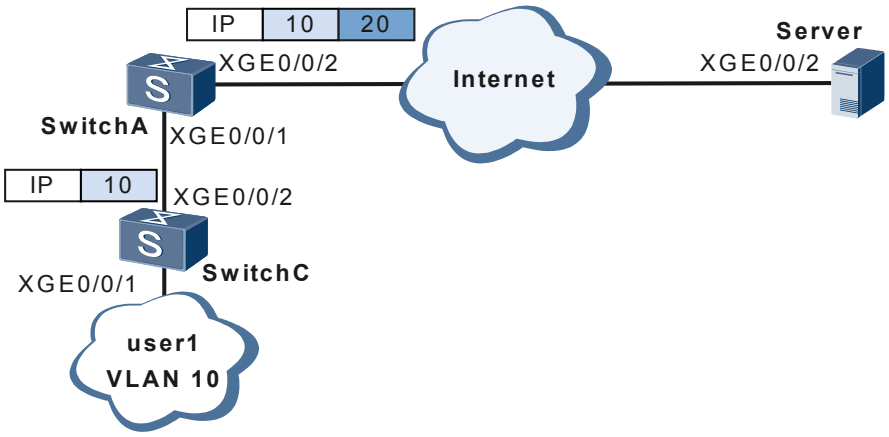
1.5.4 Example for Configuring QinQ Stacking on the VLANIF Interface

In this networking, the management VLAN is deployed on the remote server and the VLAN ID of Switch A is the same as the management VLAN ID. The VLAN ID provided by the carrier, however, is different from the management VLAN ID. To remotely log in to the remote server for managing VLAN services on Switch A, you can configure VLAN stacking according to this example.

Networking Requirements

As shown in **Figure 1-18**, Switch A is connected to the remote server through the third-party network. The management VLAN is deployed on the remote server and the VLAN ID that the downstream user connected to Switch A belongs to is the same as the management VLAN ID. The VLAN ID provided by the carrier, however, is different from the management VLAN ID.

Figure 1-18 Networking diagram for configuring QinQ stacking on the VLANIF interface



To remotely log in to the remote server for managing VLAN services on Switch A, you can configure QinQ stacking on the VLANIF interface corresponding to the management VLAN on Switch B.

NOTE

The VLANIF interface where QinQ stacking is configured must correspond to the management VLAN. This is because other types of VLANs do not support QinQ stacking.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure QinQ on Switch A.
2. Do as follows on the remote server:
   (1) Create VLAN 10 and configure VLAN 10 as the management VLAN.
   (2) Create a VLANIF interface on VLAN 10.
   (3) Configure QinQ stacking on the VLANIF interface.

Data Preparation

To complete the configuration, you need the following data:

- Outer tag that Switch A adds to data frames
- Management VLAN ID on the remote server

Procedure

Step 1 Configure Switch C.

Configure XGE 0/0/1 and XGE 0/0/2 to allow packets from VLAN 10 to pass through.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 10
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port hybrid tagged vlan 10
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] port hybrid tagged vlan 10
[SwitchC-XGigabitEthernet0/0/2] quit
```

Step 2 Configure Switch A.

Configure QinQ so that the frames sent from Switch A to the remote server carry double tags.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 20
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port vlan-stacking vlan 10 stack-vlan 20
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid tagged vlan 20
[SwitchA-XGigabitEthernet0/0/2] quit
```

Step 3 Configure the remote server.

Configure XGE 0/0/2 to allow frames from VLAN 20 to pass through.

```
<Quidway> system-view
[Quidway] sysname Server
[Server] vlan batch 10 20
[Server] interface xgigabitethernet 0/0/2
[Server-XGigabitEthernet0/0/2] port hybrid tagged vlan 20
[Server-XGigabitEthernet0/0/2] quit
```

Configure QinQ stacking.

```
[Server] vlan 10
[Server-vlan10] management-vlan
[Server-vlan10] quit
[Server] interface vlanif 10
[Server-Vlanif10] undo icmp host-unreachable send
[Server-Vlanif10] qinq stacking vlan 20
[Server-Vlanif10] ip address 10.10.10.1 24
[Server-Vlanif10] quit
[Server] interface xgigabitethernet 0/0/2
[Server-XGigabitEthernet0/0/2] port hybrid tagged vlan 10 20
```

Step 4 Verify the configuration.

You can log in to the remote server for managing VLAN services on Switch A.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
```

```
 vlan batch 20
#
interface XGigabitEthernet 0/0/1
 port hybrid untagged vlan 20
 port vlan-stacking vlan 10 stack-vlan 20
#
interface XGigabitEthernet 0/0/2
 port hybrid tagged vlan 20
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 10
#
interface XGigabitEthernet 0/0/1
 port hybrid tagged vlan 10
#
interface XGigabitEthernet 0/0/2
 port hybrid tagged vlan 10
#
return
```

- Configuration file of the remote server

```
#
 sysname Server
#
 vlan batch 10 20
#
vlan 10
 management-vlan
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
 undo icmp host-unreachable send
 qinq stacking vlan 20
#
interface XGigabitEthernet 0/0/2
 port hybrid tagged vlan 10 20
#
return
```

1.6 GVRP Configuration

This chapter describes basic concepts involved in GVRP, GVRP configuration procedures, and concludes with a GVRP configuration example.

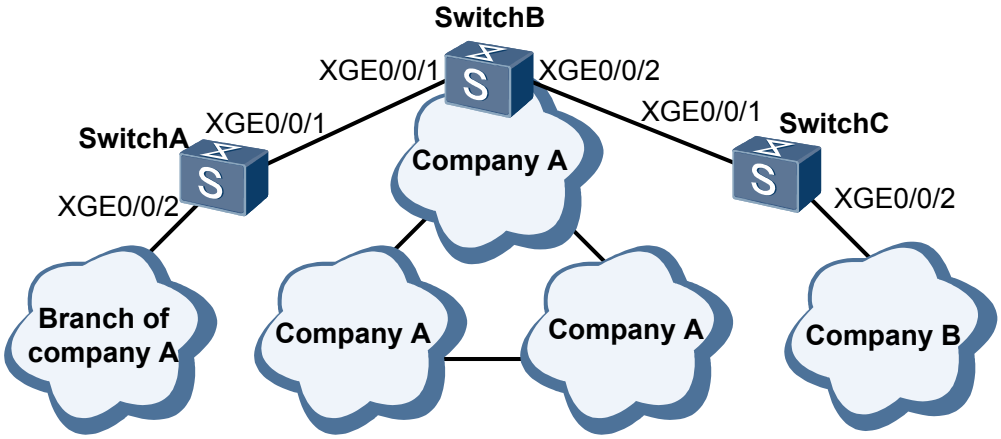
1.6.1 Example for Configuring GVRP

Networking Requirements

As shown in **Figure 1-19**, a branch of company A communicates with the headquarters through Switch A and Switch B. To simplify the configuration, you need to enable GVRP on all switches of company A and set the registration mode to normal on interfaces of these switches.

Company B communicates with company A through Switch B and Switch C. To configure switches of company B to transmit packets of only VLANs of company B, you need to enable GVRP on all switches of company B and set the registration mode to fixed on the interfaces connected to switches of company A.

Figure 1-19 Networking for configuring GVRP



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable GVRP globally.
2. Set the link type of interfaces to trunk.
3. Enable GVRP on interfaces.
4. Set the registration mode of interfaces.

Data Preparation

To complete the configuration, you need the following data:

- VLANs allowed by interfaces of Switch A, Switch B, and Switch C: all VLANs
- Registration mode of interfaces of Switch A and Switch B: normal
- Registration modes of XGE 0/0/1 and XGE 0/0/2 of Switch C: fixed and normal respectively
- VLANS of company B on Switch C: VLAN 101 to VLAN 200

Procedure

Step 1 Configure Switch A.

Enable GVRP globally.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] gvrp
```

Set the link type of XGE 0/0/1 and XGE 0/0/2 to trunk and configure the interfaces to allow all VLANs.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan all
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
```

```
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan all
[SwitchA-XGigabitEthernet0/0/2] quit
```

Enable GVRP on the interfaces and set the registration modes of the interfaces.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] gvrp
[SwitchA-XGigabitEthernet0/0/1] gvrp registration normal
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] gvrp
[SwitchA-XGigabitEthernet0/0/2] gvrp registration normal
[SwitchA-XGigabitEthernet0/0/2] bpdu enable
[SwitchA-XGigabitEthernet0/0/2] quit
```

The configuration of Switch B is similar to the configuration of Switch A, and is not mentioned here.

Step 2 Configure Switch C.

Create VLAN 101 to VLAN 200.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 101 to 200
```

Enable GVRP globally.

```
[SwitchC] gvrp
```

Set the link type of XGE 0/0/1 and XGE 0/0/2 to trunk and configure the interfaces to allow all VLANs.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port link-type trunk
[SwitchC-XGigabitEthernet0/0/1] port trunk allow-pass vlan all
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] port link-type trunk
[SwitchC-XGigabitEthernet0/0/2] port trunk allow-pass vlan all
[SwitchC-XGigabitEthernet0/0/2] quit
```

Enable GVRP on the interfaces and set the registration modes of the interfaces.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] gvrp
[SwitchC-XGigabitEthernet0/0/1] gvrp registration fixed
[SwitchC-XGigabitEthernet0/0/1] bpdu enable
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] gvrp
[SwitchC-XGigabitEthernet0/0/2] gvrp registration normal
[SwitchC-XGigabitEthernet0/0/2] bpdu enable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Step 3 Verify the configuration.

After the configuration is complete, the branch of company A can communicate with the headquarters, and users of company A in VLAN 101 to VLAN 200 can communicate with users in company B.

Run the **display gvrp status** command on Switch A to check whether GVRP is enabled globally. The following information is displayed:

```
<SwitchA> display gvrp status
 GVRP is enabled
```

Run the **display gvrp statistics** command on Switch A to view statistics about GVRP on GVRP interfaces, including the GVRP state of each interface, number of GVRP registration failures, source MAC address of the last GVRP PDU, and registration type of each interface.

```
<SwitchA> display gvrp statistics
 GVRP statistics on port XGigabitEthernet0/0/1
 GVRP status                      : Enabled
 GVRP registrations failed        : 0
 GVRP last PDU origin             : 0000-0000-0000
 GVRP registration type           : Normal
```

Verify the configurations of Switch B and Switch C in the same way.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 gvrp
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 gvrp
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 101 to 200
#
 gvrp
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
 gvrp registration fixed
#
```

```
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

1.7 MAC Address Table Configuration

This chapter provides the basics for MAC address table configuration, configuration procedure, and configuration examples.

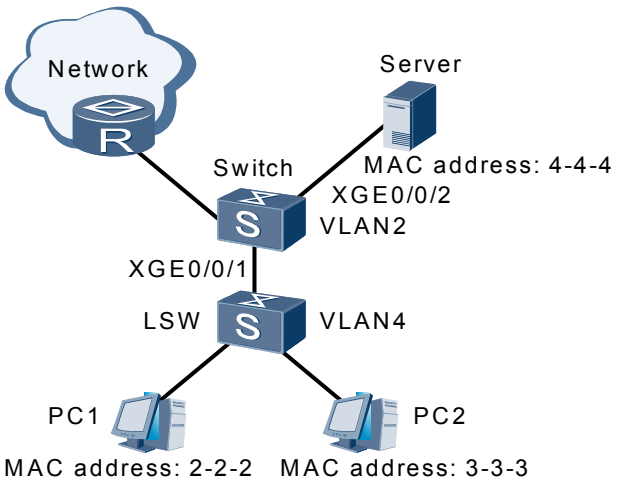
1.7.1 Example for Configuring the MAC Address Table

Networking Requirements

As shown in **Figure 1-20**, the MAC address of the user host PC1 is 0002-0002-0002 and the MAC address of the user host PC2 is 0003-0003-0003. PC1 and PC2 are connected to the Switch through the LSW. The LSW is connected to XGE 0/0/1 of the Switch. Interface XGE 0/0/1 belongs to VLAN 2. The MAC address of the server is 0004-0004-0004. The server is connected to XGE 0/0/2 of the Switch. Interface XGE 0/0/2 belongs to VLAN 2.

- To prevent hackers from attacking the network with MAC addresses, you need to add a static entry to the MAC table of the Switch for each user host. When sending packets through XGE 0/0/1, the Switch changes the VLAN ID to VLAN 4 to which the LSW belongs. In addition, you need to set the aging time of the dynamic entries in the MAC address table to 500 seconds.
- To prevent hackers from forging the MAC address of the server and stealing user information, you can configure the packet forwarding based on static MAC address entries on the Switch.

Figure 1-20 Networking diagram for configuring the MAC address table



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and add interfaces to the VLAN.
2. Add static MAC address entries.
3. Set the aging time of dynamic MAC address entries.

Data Preparation

To complete the configuration, you need the following data:

- MAC address of PC1: 0002-0002-0002
- MAC address of PC2: 0003-0003-0003
- MAC address of the server: 0004-0004-0004
- VLAN to which the Switch belongs: VLAN 2
- Interface connecting the Switch to the LSW: XGE 0/0/1
- Interface connecting the Switch to the server: XGE 0/0/2
- VLAN ID required to be changed to when the Switch sends packets through the outgoing interface: VLAN 4
- Aging time of dynamic entries in the MAC address table of the Switch: 500 seconds

Procedure

Step 1 Add static MAC address entries.

Create VLAN 2; add XGE 0/0/1 0/0/2 to VLAN 2; configure VLAN mapping on XGE 0/0/1.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 2
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 2
[Quidway-XGigabitEthernet0/0/1] qinq  vlan-translation  enable
[Quidway-XGigabitEthernet0/0/1] port vlan-mapping vlan 4 map-vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 2
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 2
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure static MAC address entries.

```
[Quidway] mac-address static 2-2-2 xgigabitethernet 0/0/1 vlan 2
[Quidway] mac-address static 3-3-3 xgigabitethernet 0/0/1 vlan 2
[Quidway] mac-address static 4-4-4 xgigabitethernet 0/0/2 vlan 2
```

Step 2 Set the aging time of dynamic MAC address entries.

```
[Quidway] mac-address aging-time 500
```

Step 3 Verify the configuration.

Run the **display mac-address static** command in any view. You can check whether the static MAC address entries are successfully added.

```
[Quidway] display mac-address static vlan 2
--------------------------------------------------------------------------------
```

```
MAC Address          VLAN/VSI                    Learned-From        Type
------------------------------------------------------------------------------
0002-0002-0002       2/-                         XGE0/0/1            static
0003-0003-0003       2/-                         XGE0/0/1            static
0004-0004-0004       2/-                         XGE0/0/2            static
------------------------------------------------------------------------------
Total items displayed  = 3
```

Run the **display mac-address aging-time** command in any view. You can check whether the aging time of dynamic entries is set successfully.

```
[Quidway] display mac-address aging-time
  Aging time: 500 seconds
```

----End

Configuration Files

The following lists the configuration file of the Switch.

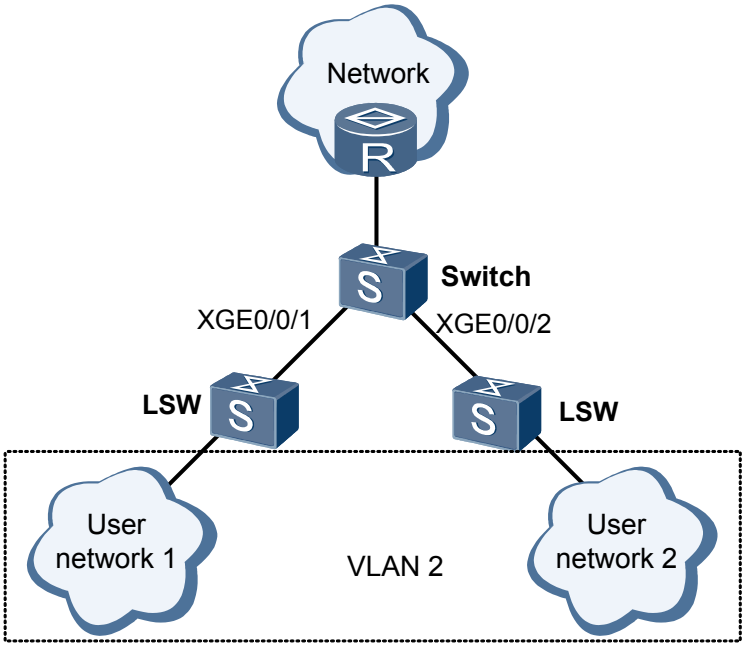
```
#
 sysname Quidway
#
 vlan batch 2
#
 mac-address aging-time 500
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
 qinq  vlan-translation  enable
 port vlan-mapping vlan 4 map-vlan 2
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
 mac-address static 0002-0002-0002 XGigabitEthernet0/0/1 vlan 2
 mac-address static 0003-0003-0003 XGigabitEthernet0/0/1 vlan 2
 mac-address static 0004-0004-0004 XGigabitEthernet0/0/2 vlan 2
#
return
```

1.7.2 Example for Configuring the Limitation on MAC Address Learning Based on VLANs

Networking Requirements

As shown in **Figure 1-21**, user network 1 is connected to XGE 0/0/1 on the Switch through an LSW. User network 2 is connected to XGE 0/0/2 on the Switch through another LSW. XGE 0/0/1 and XGE 0/0/2 belong to VLAN 2. To prevent MAC address attacks and control the number of access users, you need to limit the MAC address learning in VLAN 2.

Figure 1-21 Networking diagram for configuring the limitation on MAC address learning based on VLAN



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and add interfaces to the VLAN.
2. Configure the limitation on MAC address learning based on VLANs.

Data Preparation

To complete the configuration, you need the following data:

- VLAN to which the interfaces belong: VLAN 2
- User interfaces: XGE 0/0/1 and XGE 0/0/2
- Maximum number of learned MAC addresses: 100

Procedure

Step 1 Configure the limitation on MAC address learning.

Add XGE 0/0/1 and XGE 0/0/2 to VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 2
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 2
```

```
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 2
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure the rule of limiting MAC address learning in VLAN 2: A maximum of 100 MAC addresses can be learned; packets are still forwarded and an alarm is generated when the number of learned MAC addresses reaches the limit, but new MAC addresses are not added to the MAC address table.

```
[Quidway] vlan 2
[Quidway-vlan2] mac-limit maximum 100 alarm enable
[Quidway-vlan2] quit
```

Step 2 Verify the configuration.

Run the **display mac-limit** command in any view. You can check whether the rule of limiting MAC address learning is successfully configured.

```
<Quidway> display mac-limit
MAC Limit is enabled
Total MAC Limit rule count : 1

PORT                 VLAN/VSI/SI      SLOT Maximum Rate(ms) Action  Alarm
-------------------------------------------------------------------------------
-                    2                -    100     -        forward enable
```

----End

Configuration Files

The following lists the configuration file of the Switch.

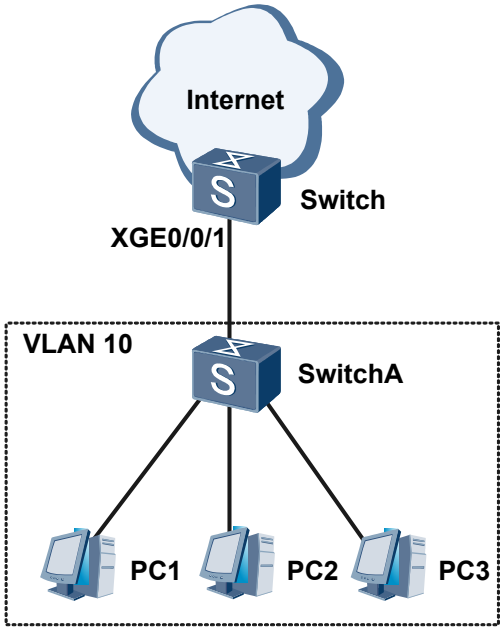
```
#
 sysname Quidway
#
 vlan batch 2
#
vlan 2
 mac-limit maximum 100
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
return
```

1.7.3 Example for Configuring Interface Security

Networking Requirements

As shown in **Figure 1-22**, a company wants to prevent the computers of non-employees from accessing the intranet of the company to protect information security. To achieve this goal, the company needs to enable the sticky MAC function on the interface connected to computers of employees and set the maximum number of MAC addresses learned by the interface to be the same as the number of trusted computers.

Figure 1-22 Networking diagram of interface security configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and set the link type of the interface to trunk.
2. Enable the interface security function.
3. Enable the sticky MAC function on the interface.
4. Configure the security protection action on the interface.
5. Set the maximum number of MAC addresses that can be learned by the interface.

Data Preparation

To complete the configuration, you need the following data:

- VLAN allowed by the interface
- Type and number of the interface connected to computers of employees
- Security protection action
- Maximum number of MAC addresses learned by the interface

Procedure

Step 1 Create a VLAN and set the link type of the interface to trunk.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type trunk
[Quidway-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
```

Step 2 Configure the interface security function.

Enable the interface security function.

```
[Quidway-XGigabitEthernet0/0/1] port-security enable
```

Enable the sticky MAC function.

```
[Quidway-XGigabitEthernet0/0/1] port-security mac-address sticky
```

Configure the security protection action.

```
[Quidway-XGigabitEthernet0/0/1] port-security protect-action protect
```

Set the maximum number of MAC addresses that can be learned by the interface.

```
[Quidway-XGigabitEthernet0/0/1] port-security max-mac-num 4
```

To enable the interface security function on other interfaces, repeat the preceding steps.

Step 3 Verify the configuration.

If PC1 is replaced by another PC, this PC cannot access the intranet of the company.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 port-security enable
 port-security protect-action protect
 port-security mac-address sticky
 port-security max-mac-num 4
#
return
```

1.7.4 Example for Configuring MAC Address Anti-Flapping

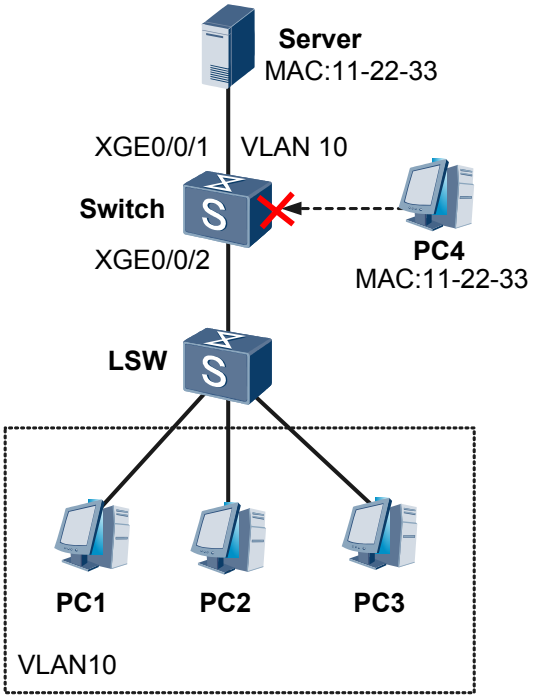
The MAC address anti-flapping function protects servers of an enterprise or VIP customers from attacks.

Networking Requirements

As shown in **Figure 1-23**, employees of an enterprise need to access the server connected to a Switch interface. If an attacker uses the server MAC address as the source MAC address to send packets to another interface, the server MAC address is learned on the interface. Employees cannot access the server, and important data will be intercepted by the attacker.

MAC address anti-flapping can be configured to protect the server from attacks.

Figure 1-23 Networking diagram for MAC address anti-flapping



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and add interfaces to the VLAN.
2. Configure MAC address anti-flapping on the server-side interface.

Data Preparation

To complete the configuration, you need the following data:

- VLAN that the server-side and user-side interfaces belong to: VLAN 10
- Server-side interface: XGigabitEthernet0/0/1
- User-side interface: XGigabitEthernet0/0/2
- MAC address learning priority of the server-side interface: 2

Procedure

Step 1 Create a VLAN and add interfaces to the VLAN.

Add XGigabitEthernet0/0/1 and XGigabitEthernet0/0/2 to VLAN 10.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type trunk
[Quidway-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Quidway-XGigabitEthernet0/0/2] quit
```

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
```

Step 2 Configure MAC anti-flapping.

Set the MAC address learning priority of XGigabitEthernet0/0/1 to 2.

```
[Quidway-XGigabitEthernet0/0/1] mac-learning priority 2
```

Step 3 Verify the configuration.

Run the **display current-configuration** command in any view to check whether the MAC address learning priority of XGigabitEthernet0/0/1 is set correctly.

```
<Quidway> display current-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mac-learning priority 2
#
return
```

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mac-learning priority 2
#
interface XGigabitEthernet0/0/2
 port link-type  trunk
 port trunk allow-pass vlan 10
#
return
```

1.8 STP/RSTP Configuration

The Spanning Tree Protocol (STP) trims a ring network into a loop-free tree network. It prevents replication and circular propagation of packets, provides multiple redundant paths for Virtual LAN (VLAN) data traffic, and enables load balancing. The Rapid Spanning Tree Protocol (RSTP) develops rapid convergence and introduces the edge port and its protection function based on STP.

1.8.1 Example for Configuring Basic STP Functions

This example shows how to configure basic STP functions.

Networking Requirements

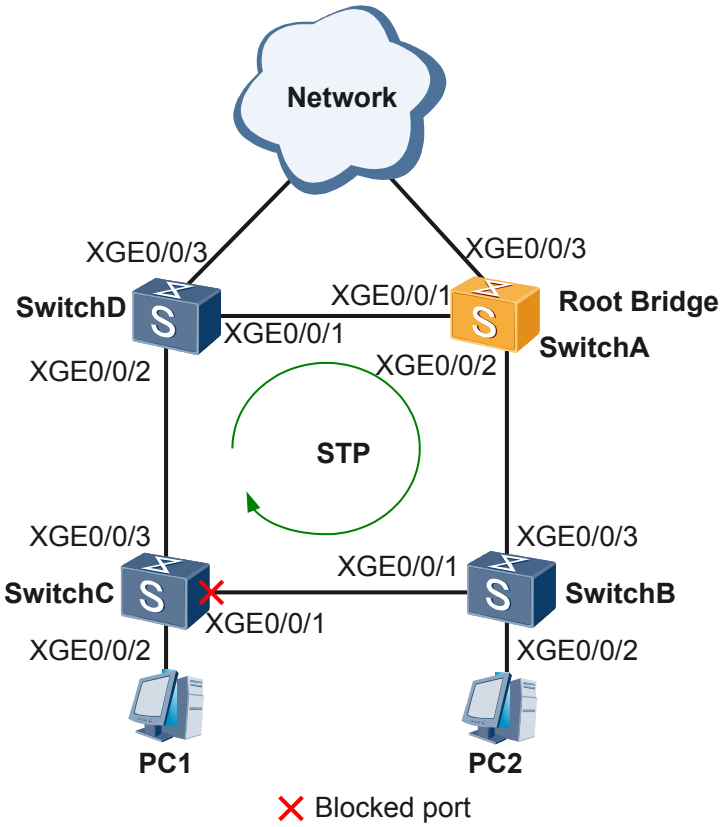
On a complex network, loops are inevitable. With the requirement for network redundancy backup, network designers tend to deploy multiple physical links between two devices, one of

which is the master and the others are the backup. Loops are likely or bound to occur in such a situation.

Loops will cause broadcast storms, thereby exhausting network resources and paralyzing the network. Loops also cause flapping of MAC address tables and damages MAC address entries.

STP can be deployed on a network to eliminate loops by blocking some ports. On the network shown in **Figure 1-24**, after SwitchA, SwitchB, SwitchC, and SwitchD running STP discover loops on the network by exchanging information with each other, they trim the ring topology into a loop-free tree topology by blocking a certain port. In this manner, replication and circular propagation of packets are prevented on the network and the switching devices are released from processing duplicated packets, thereby improving their processing performance.

Figure 1-24 Networking diagram of configuring basic STP functions



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic STP functions, including:
   (1) Configure the STP mode for the ring network.
   (2) Configure primary and secondary root bridges.
   (3) Set path costs for ports to block certain ports.
   (4) Enable STP to eliminate loops.

NOTE

STP is not required on the interfaces connected to terminals because these interfaces do not need to participate in STP calculation.

Data Preparation

To complete the configuration, you need the following data:

- XGEInterface number, as shown in **Figure 1-24**
- Primary root bridge SwitchA and secondary root bridge SwitchD
- Path cost of a port to be blocked (20000 is used in this example)

Procedure

Step 1 Configure basic STP functions.

1. Configure the STP mode for the devices on the ring network.

   # Configure the STP mode on SwitchA.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchA
   [SwitchA] stp mode stp
   ```

   # Configure the STP mode on SwitchB.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchB
   [SwitchB] stp mode stp
   ```

   # Configure the STP mode on SwitchC.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchC
   [SwitchC] stp mode stp
   ```

   # Configure the STP mode on SwitchD.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchD
   [SwitchD] stp mode stp
   ```

2. Configure primary and secondary root bridges.

   # Configure SwitchA as a primary root bridge.

   ```
   [SwitchA] stp root primary
   ```

   # Configure SwitchD as a secondary root bridge.

   ```
   [SwitchD] stp root secondary
   ```

3. Set path costs for ports in each spanning tree to block certain ports.

   NOTE

   - The values of path costs depend on path cost calculation methods. Use the Huawei proprietary calculation method as an example to set the path costs of the ports to be blocked to 20000.
   - All switching devices on a network must use the same path cost calculation method.

   # Set the path cost of XGE0/0/1 on SwitchC to 20000.

   ```
   [SwitchC] interface xgigabitethernet 0/0/1
   [SwitchC-XGigabitEthernet0/0/1] stp cost 20000
   [SwitchC-XGigabitEthernet0/0/1] quit
   ```

4. Enable STP to eliminate loops.

   - Disable STP on interfaces connected to PCs.

     # Disable STP on XGE 0/0/2 on SwitchB.

     ```
     [SwitchB] interface xgigabitethernet 0/0/2
     ```

```
[SwitchB-XGigabitEthernet0/0/2] stp disable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Disable STP on XGE 0/0/2 on SwitchC.

```
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] stp disable
[SwitchC-XGigabitEthernet0/0/2] quit
```

- Enable STP globally.

  # Enable STP globally on SwitchA.

  ```
  [SwitchA] stp enable
  ```

  # Enable STP globally on SwitchB.

  ```
  [SwitchB] stp enable
  ```

  # Enable STP globally on SwitchC.

  ```
  [SwitchC] stp enable
  ```

  # Enable STP globally on SwitchD.

  ```
  [SwitchD] stp enable
  ```

- Enable BPDU on all the interfaces except the interfaces connected to terminals.

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/2 on SwitchA.

  ```
  [SwitchA] interface xgigabitethernet 0/0/1
  [SwitchA-XGigabitEthernet0/0/1] bpdu enable
  [SwitchA-XGigabitEthernet0/0/1] quit
  [SwitchA] interface xgigabitethernet 0/0/2
  [SwitchA-XGigabitEthernet0/0/2] bpdu enable
  [SwitchA-XGigabitEthernet0/0/2] quit
  ```

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/3 on SwitchB.

  ```
  [SwitchB] interface xgigabitethernet 0/0/1
  [SwitchB-XGigabitEthernet0/0/1] bpdu enable
  [SwitchB-XGigabitEthernet0/0/1] quit
  [SwitchB] interface xgigabitethernet 0/0/3
  [SwitchB-XGigabitEthernet0/0/3] bpdu enable
  [SwitchB-XGigabitEthernet0/0/3] quit
  ```

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/3 on SwitchC.

  ```
  [SwitchC] interface xgigabitethernet 0/0/1
  [SwitchC-XGigabitEthernet0/0/1] bpdu enable
  [SwitchC-XGigabitEthernet0/0/1] quit
  [SwitchC] interface xgigabitethernet 0/0/3
  [SwitchC-XGigabitEthernet0/0/3] bpdu enable
  [SwitchC-XGigabitEthernet0/0/3] quit
  ```

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/2 on SwitchD.

  ```
  [SwitchD] interface xgigabitethernet 0/0/1
  [SwitchD-XGigabitEthernet0/0/1] bpdu enable
  [SwitchD-XGigabitEthernet0/0/1] quit
  [SwitchD] interface xgigabitethernet 0/0/2
  [SwitchD-XGigabitEthernet0/0/2] bpdu enable
  [SwitchD-XGigabitEthernet0/0/2] quit
  ```

Step 2 Verify the configuration.

After the previous configurations, run the following commands to verify the configuration when the network is stable:

Run the **display stp brief** command on SwitchA to view the interface status and protection type. The displayed information is as follows:

```
[SwitchA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1       DESI  FORWARDING      NONE
   0    XGigabitEthernet0/0/2       DESI  FORWARDING      NONE
```

After SwitchA is configured as a root bridge, XGE 0/0/2 and XGE 0/0/1 connected to SwitchB and SwitchD respectively are elected as designated ports in spanning tree calculation.

Run the **display stp interface xgigabitethernet 0/0/1 brief** command on SwitchB to view status of XGE 0/0/1. The displayed information is as follows:

```
[SwitchB] display stp interface xgigabitethernet 0/0/1 brief
 MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1        DESI  FORWARDING      NONE
```

XGE 0/0/1 is elected as a designated port in spanning tree calculation and is in the Forwarding state.

Run the **display stp brief** command on SwitchC to view the interface status and protection type. The displayed information is as follows:

```
[SwitchC] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    XGigabitEthernet0/0/3        ROOT  FORWARDING      NONE
```

XGE 0/0/1 is elected as an alternate port in spanning tree calculation and is in the Discarding state.

XGE 0/0/3 is elected as a root port in spanning tree calculation and is in the Forwarding state.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname
SwitchA
#
 stp mode
stp
 stp instance 0 root
primary
#
return
```

- Configuration file of SwitchB

```
#
 sysname
SwitchB
#
 stp mode
stp
#
interface XGigabitEthernet0/0/2
 stp disable
#
return
```

- Configuration file of SwitchC

```
#
 sysname
SwitchC
#
 stp mode
stp
#
interface XGigabitEthernet0/0/1
 stp instance 0 cost
20000
```

```
#
interface XGigabitEthernet0/0/2
 stp disable
#
return
```

- Configuration file of SwitchD

```
#
 sysname
SwitchD
#
 stp mode
stp
 stp instance 0 root
secondary
#
return
```

1.8.2 Example for Configuring Basic RSTP Functions

This example describes how to configure basic RSTP functions.

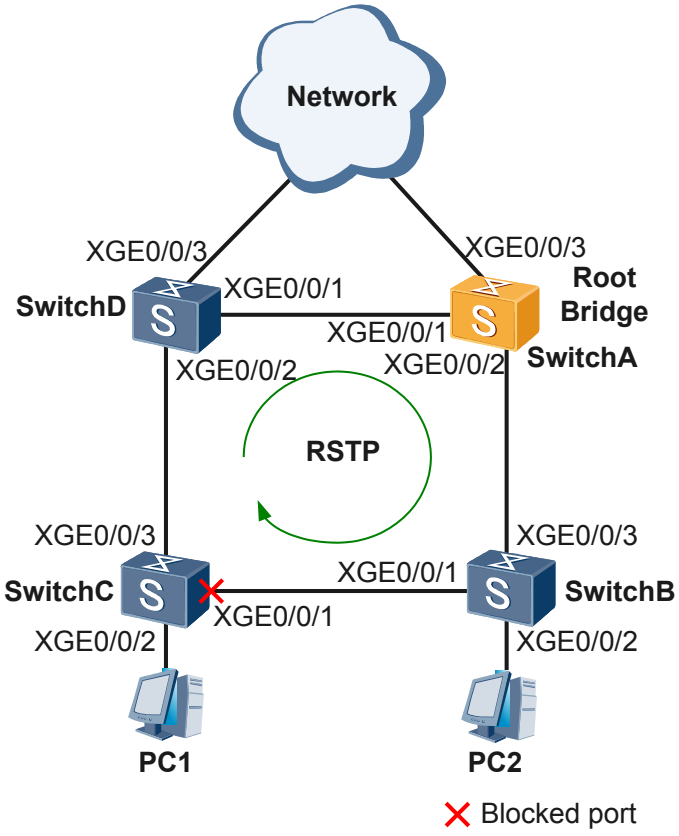
Networking Requirements

On a complex network, loops often occur. To implement network redundancy backup, network designers tend to deploy multiple physical links between two devices, one of which is the master device and the others are backup devices. Loops are likely or bound to occur in such a situation.

Loops will cause broadcast storms, exhausting network resources and making the network break down. Loops also cause flapping of MAC address tables and damage MAC address entries.

RSTP can be deployed on a network to eliminate loops by blocking some ports. On the network shown in **Figure 1-25**, after SwitchA, SwitchB, SwitchC, and SwitchD running RSTP detect loops on the network by exchanging information with each other, they trim the ring topology into a loop-free tree topology by blocking a certain port. In this manner, packets are not replicated and looped on the network and switching devices do not need to process duplicate packets, improving their processing performance.

Figure 1-25 Networking diagram of basic RSTP functions



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic RSTP functions, including:
   (1) Configure the RSTP mode for the ring network.
   (2) Configure primary and secondary root bridges.
   (3) Set path costs for ports in each MSTI to block certain ports.
   (4) Enable RSTP to eliminate loops.

   NOTE

   RSTP is not required on the interfaces connected to terminals because these interfaces do not need to participate in RSTP calculation.
2. Configure RSTP protection functions, for example, root protection on a designated port of a root bridge in each MSTI.

Data Preparation

To complete the configuration, you need the following data:

- XGE interface number, as shown in **Figure 1-25**
- Primary root bridge SwitchA and secondary root bridge SwitchD

- Path cost of a port to be blocked (20000 is used in this example)

Procedure

Step 1 Configure basic RSTP functions.

1. Configure the RSTP mode for the devices on the ring network.

   # Configure the RSTP mode on SwitchA.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchA
   [SwitchA] stp mode rstp
   ```

   # Configure the RSTP mode on SwitchB.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchB
   [SwitchB] stp mode rstp
   ```

   # Configure the RSTP mode on SwitchC.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchC
   [SwitchC] stp mode rstp
   ```

   # Configure the RSTP mode on SwitchD.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchD
   [SwitchD] stp mode rstp
   ```

2. Configure primary and secondary root bridges.

   # Configure SwitchA as a primary root bridge.

   ```
   [SwitchA] stp root primary
   ```

   # Configure SwitchD as a secondary root bridge.

   ```
   [SwitchD] stp root secondary
   ```

3. Set path costs for ports to block certain ports.

   NOTE

   - The values of path costs depend on path cost calculation methods. Use the Huawei proprietary calculation method as an example to set the path costs of the ports to be blocked to 20000.
   - All switching devices on a network must use the same path cost calculation method.

   # Set the path cost of XGE0/0/1 on SwitchC to 20000.

   ```
   [SwitchC] interface xgigabitethernet 0/0/1
   [SwitchC-XGigabitEthernet0/0/1] stp cost 20000
   [SwitchC-XGigabitEthernet0/0/1] quit
   ```

4. Enable RSTP to eliminate loops.

   - Disable RSTP on interfaces connected to PCs.

     # Disable RSTP on XGE 0/0/2 on SwitchB.

     ```
     [SwitchB] interface xgigabitethernet 0/0/2
     [SwitchB-XGigabitEthernet0/0/2] stp disable
     [SwitchB-XGigabitEthernet0/0/2] quit
     ```

     # Disable RSTP on XGE 0/0/2 on SwitchC.

     ```
     [SwitchC] interface xgigabitethernet 0/0/2
     [SwitchC-XGigabitEthernet0/0/2] stp disable
     [SwitchC-XGigabitEthernet0/0/2] quit
     ```

   - Enable RSTP globally.

     # Enable RSTP globally on SwitchA.

     ```
     [SwitchA] stp enable
     ```

     # Enable RSTP globally on SwitchB.

```
[SwitchB] stp enable
```

Enable RSTP globally on SwitchC.

```
[SwitchC] stp enable
```

Enable RSTP globally on SwitchD.

```
[SwitchD] stp enable
```

- Enable BPDU on all the interfaces except the interfaces connected to terminals.

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/2 on SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] bpdu enable
[SwitchA-XGigabitEthernet0/0/2] quit
```

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/3 on SwitchB.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] bpdu enable
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/3
[SwitchB-XGigabitEthernet0/0/3] bpdu enable
[SwitchB-XGigabitEthernet0/0/3] quit
```

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/3 on SwitchC.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] bpdu enable
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/3
[SwitchC-XGigabitEthernet0/0/3] bpdu enable
[SwitchC-XGigabitEthernet0/0/3] quit
```

  # Enable BPDU on XGE 0/0/1 and XGE 0/0/2 on SwitchD.

```
[SwitchD] interface xgigabitethernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] bpdu enable
[SwitchD-XGigabitEthernet0/0/1] quit
[SwitchD] interface xgigabitethernet 0/0/2
[SwitchD-XGigabitEthernet0/0/2] bpdu enable
[SwitchD-XGigabitEthernet0/0/2] quit
```

Step 2 Configure RSTP protection functions.

Enable root protection on XGE 0/0/1 on SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] stp root-protection
[SwitchA-XGigabitEthernet0/0/1] quit
```

Enable root protection on XGE 0/0/2 on SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp root-protection
[SwitchA-XGigabitEthernet0/0/2] quit
```

Step 3 Verify the configuration.

After the previous configurations, run the following commands to verify the configuration when the network is stable:

Run the **display stp brief** command on SwitchA to view the interface status and protection type. The displayed information is as follows:

```
[SwitchA] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1        DESI  FORWARDING      ROOT
   0    XGigabitEthernet0/0/2        DESI  FORWARDING      ROOT
```

After SwitchA is configured as a root bridge, XGE 0/0/2 and XGE 0/0/1 connected to SwitchB and SwitchD respectively are elected as designated ports in spanning tree calculation. The root protection function is enabled on the designated ports.

Run the **display stp interface xgigabitethernet 0/0/1 brief** command on SwitchB to view status of XGE 0/0/1. The displayed information is as follows:

```
[SwitchB] display stp interface xgigabitethernet 0/0/1 brief
 MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1        DESI  FORWARDING      NONE
```

XGE 0/0/1 is elected as a designated port in spanning tree calculation and is in the Forwarding state.

Run the **display stp brief** command on SwitchC to view the interface status and protection type. The displayed information is as follows:

```
[SwitchC] display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    XGigabitEthernet0/0/3        ROOT  FORWARDING      NONE
```

XGE 0/0/1 is elected as an alternate port in spanning tree calculation and is in the Discarding state.

XGE 0/0/3 is elected as a root port in spanning tree calculation and is in the Forwarding state.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 stp mode
rstp
 stp instance 0 root
primary
#
interface XGigabitEthernet0/0/1
 stp root-
protection
#
interface XGigabitEthernet0/0/2
 stp root-
protection
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 stp mode
rstp
#
interface XGigabitEthernet0/0/2
 stp disable
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
```

```
 stp mode
rstp
#
interface XGigabitEthernet0/0/1
 stp instance 0 cost
20000
#
interface XGigabitEthernet0/0/2
 stp disable
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 stp mode
rstp
 stp instance 0 root
secondary
#
return
```

1.9 MSTP Configuration

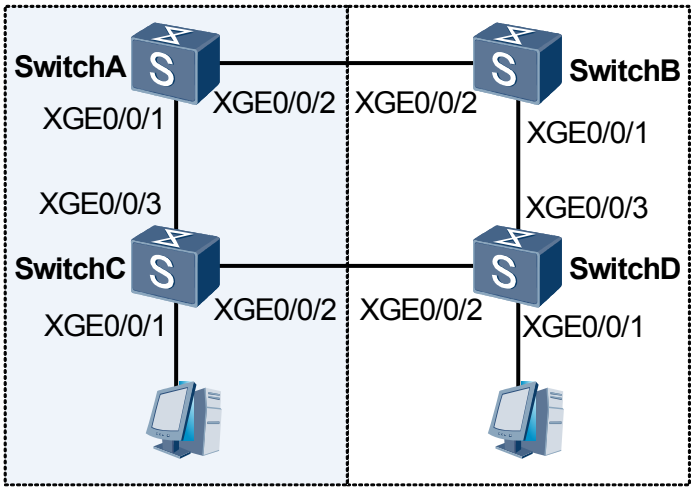
The Multiple Spanning Tree Protocol (MSTP) trims a ring network into a loop-free tree network. It prevents replication and circular propagation of packets, provides multiple redundant paths for Virtual LAN (VLAN) data traffic, and enables load balancing.

1.9.1 Example for Configuring Basic MSTP Functions

Networking Requirements

SwitchA, SwitchB, SwitchC, and SwitchD run MSTP. In this example, MSTP runs on Layer 2 interfaces of the Switches.

Figure 1-26 Networking diagram of basic MSTP configurations



Configuration Roadmap

The configuration roadmap is as follows:

1. Add SwitchA and SwitchC to MST region RG1, and create MSTI1.
2. Add SwitchB and SwitchD to MST region RG2, and create MSTI1.
3. Configure SwitchA as the CIST root.
4. In RG1, configure SwitchA as the CIST regional root and regional root of MSTI1. Configure the root protection function on XGE 0/0/2 and the XGE 0/0/1 on SwitchA.
5. In RG2, configure SwitchB as the CIST regional root and SwitchD as the regional root of MSTI1.
6. On SwitchC and SwitchD, connect XGE 0/0/1 to a PC and configure XGE 0/0/1 as an edge port. Enable BPDU protection on SwitchC and SwitchD.
7. Configure the Switches to calculate the path cost by using the algorithm of Huawei.

Data Preparation

To complete the configuration, you need the following data:

- Region that SwitchA and SwitchC belong to: RG1
- Region that SwitchB and SwitchD belong to: RG2
- Numbers of the XGE interfaces, as shown in **Figure 1-26**
- VLAN IDs: 1-20

Procedure

Step 1 Configure SwitchA.

Configure the MST region on SwitchA.

```
<SwitchA> system-view
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name RG1
[SwitchA-mst-region] instance 1 vlan 1 to 10
```

Activate the configuration of the MST region.

```
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

Set the priority of SwitchA in MSTI0 to 0 to ensure that SwitchA functions as the CIST root.

```
[SwitchA] stp instance 0 priority 0
```

Set the priority of SwitchA in MSTI1 to 1 to ensure that SwitchA functions as the regional root of MSTI1.

```
[SwitchA] stp instance 1 priority 0
```

Configure SwitchA to use Huawei private algorithm to calculate the path cost.

```
[SwitchA] stp pathcost-standard legacy
```

Create VLANs 2 to 20.

```
[SwitchA] vlan batch 2 to 20
```

Add XGE 0/0/2 to the VLANs.

```
[SwitchA] interface XGigabitEthernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchA-XGigabitEthernet0/0/2] bpdu enable
[SwitchA-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/1 to the VLANs.

```
[SwitchA] interface XGigabitEthernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 1 to 20
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
[SwitchA-XGigabitEthernet0/0/1] quit
```

Enable root protection on the XGE 0/0/1.

```
[SwitchA] interface XGigabitEthernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] stp root-protection
[SwitchA-XGigabitEthernet0/0/1] quit
```

Enable root protection on the XGE 0/0/2.

```
[SwitchA] interface XGigabitEthernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp root-protection
[SwitchA-XGigabitEthernet0/0/2] quit
```

Enable MSTP.

```
[SwitchA] stp enable
```

Step 2 Configure SwitchB.

Configure the MST region on SwitchB.

```
[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name RG2
[SwitchB-mst-region] instance 1 vlan 1 to 10
```

Activate the configuration of the MST region.

```
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

Set the priority of SwitchB in MSTI0 to 4096 to ensure that SwitchB functions as the CIST root.

```
[SwitchB] stp instance 0 priority 4096
```

Configure SwitchB to use Huawei private algorithm to calculate the path cost.

```
[SwitchB] stp pathcost-standard legacy
```

Create VLANs 2 to 20.

```
[SwitchB] vlan batch 2 to 20
```

Add XGE 0/0/1 to the VLANs.

```
[SwitchB] interface XGigabitEthernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 1 to 20
[SwitchB-XGigabitEthernet0/0/1] bpdu enable
[SwitchB-XGigabitEthernet0/0/1] quit
```

Add XGE 0/0/2 to the VLANs.

```
[SwitchB] interface XGigabitEthernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] port link-type trunk
[SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
```

```
[SwitchB-XGigabitEthernet0/0/2] bpdu enable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Enable MSTP.

```
[SwitchB] stp enable
```

Step 3 Configure SwitchC.

Configure the MST region on SwitchC.

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] region-name RG1
[SwitchC-mst-region] instance 1 vlan 1 to 10
```

Activate the configuration of the MST region.

```
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
```

Configure SwitchC to use Huawei private algorithm to calculate the path cost.

```
[SwitchC] stp pathcost-standard legacy
```

Enable BPDU protection.

```
[SwitchC] stp bpdu-protection
```

Create VLANs 2 to 20.

```
[SwitchC] vlan batch 2 to 20
```

Add XGE 0/0/2 to the VLANs.

```
[SwitchC] interface XGigabitEthernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] port link-type trunk
[SwitchC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchC-XGigabitEthernet0/0/2] bpdu enable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/3 to the VLANs.

```
[SwitchC] interface XGigabitEthernet 0/0/3
[SwitchC-XGigabitEthernet0/0/3] port link-type trunk
[SwitchC-XGigabitEthernet0/0/3] port trunk allow-pass vlan 1 to 20
[SwitchC-XGigabitEthernet0/0/3] bpdu enable
[SwitchC-XGigabitEthernet0/0/3] quit
```

Configure XGE 0/0/1 as an edge port.

```
[SwitchC] interface XGigabitEthernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] stp edged-port enable
[SwitchC-XGigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchC-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchC-XGigabitEthernet0/0/1] quit
```

Enable MSTP.

```
[SwitchC] stp enable
```

Step 4 Configure SwitchD.

Configure the MST region on SwitchD.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] region-name RG2
[SwitchD-mst-region] instance 1 vlan 1 to 10
```

Activate the configuration of the MST region.

```
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

Set the priority of SwitchD in MSTI1 to 0 to ensure that SwitchD functions as the regional root of MSTI1.

```
[SwitchD] stp instance 1 priority 0
```

Configure SwitchD to use Huawei private algorithm to calculate the path cost.

```
[SwitchD] stp pathcost-standard legacy
```

Enable BPDU protection.

```
[SwitchD] stp bpdu-protection
```

Create VLANs 2 to 20.

```
[SwitchD] vlan batch 2 to 20
```

Add XGE 0/0/2 to the VLANs.

```
[SwitchD] interface XGigabitEthernet 0/0/2
[SwitchD-XGigabitEthernet0/0/2] port link-type trunk
[SwitchD-XGigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[SwitchD-XGigabitEthernet0/0/2] bpdu enable
[SwitchD-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/3 to the VLANs.

```
[SwitchD] interface XGigabitEthernet 0/0/3
[SwitchD-XGigabitEthernet0/0/3] port link-type trunk
[SwitchD-XGigabitEthernet0/0/3] port trunk allow-pass vlan 1 to 20
[SwitchD-XGigabitEthernet0/0/3] bpdu enable
[SwitchD-XGigabitEthernet0/0/3] quit
```

Configure XGE 0/0/1 as an edge port.

```
[SwitchD] interface XGigabitEthernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] stp edged-port enable
[SwitchD-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchD-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchD-XGigabitEthernet0/0/1] quit
```

Enable MSTP.

```
[SwitchD] stp enable
```

Step 5 Verify the configuration.

After the preceding configurations are complete and the network topology becomes stable, perform the following operations to verify the configuration.

Run the **display stp brief** command on SwitchA to view the status and protection type on the interfaces. The displayed information is as follows:

```
<SwitchA> display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        XGigabitEthernet0/0/1  DESI  FORWARDING      ROOT
   0        XGigabitEthernet0/0/2  DESI  FORWARDING      ROOT
   1        XGigabitEthernet0/0/1  DESI  FORWARDING      ROOT
   1        XGigabitEthernet0/0/2  DESI  FORWARDING      ROOT
```

The priority of SwitchA is the highest in the CIST; therefore, SwitchA is elected as the CIST root and regional root of RG1. XGE 0/0/2 and XGE 0/0/1 of SwitchA are designated ports in the CIST.

The priority of SwitchA in MSTI1 is the highest in RG1; therefore, SwitchA is elected as the regional root of SwitchA. XGE 0/0/2 and XGE 0/0/1 of SwitchA are designated ports in MSTI1.

Run the **display stp interface brief** commands on SwitchC. The displayed information is as follows:

```
<SwitchC> display stp interface XGigabitEthernet 0/0/3 brief
 MSTID      Port                    Role  STP State     Protection
   0        XGigabitEthernet0/0/3    ROOT  FORWARDING      NONE
   1        XGigabitEthernet0/0/3    ROOT  FORWARDING      NONE
<SwitchC> display stp interface XGigabitEthernet 0/0/2 brief
 MSTID      Port                    Role  STP State     Protection
   0        XGigabitEthernet0/0/2    DESI  FORWARDING      NONE
   1        XGigabitEthernet0/0/2    DESI  FORWARDING      NONE
```

XGE 0/0/3 of SwitchC is the root port in the CIST and MSTI1. XGE 0/0/2 of SwitchC is a designated port in the CIST and MSTI1.

Run the **display stp brief** command on SwitchB. The displayed information is as follows:

```
<SwitchB> display stp brief
 MSTID      Port                  Role  STP State     Protection
   0        XGigabitEthernet0/0/1  DESI  FORWARDING      NONE
   0        XGigabitEthernet0/0/2  ROOT  FORWARDING      NONE
   1        XGigabitEthernet0/0/1  ROOT  FORWARDING      NONE
   1        XGigabitEthernet0/0/2  MAST  FORWARDING      NONE
```

The priority of SwitchB in the CIST is lower than that of SwitchA; therefore, XGE 0/0/2 of SwitchB functions as the root port in the CIST. SwitchA and SwitchB belong to different regions; therefore, XGE 0/0/2 of SwitchB functions as the master port in MSTI1. In MSTI1, the priority of SwitchB is lower than that of SwitchD; therefore, XGE 0/0/1 of SwitchB functions as the root port. The priority of SwitchB in the CIST is higher than that of SwitchB; therefore, XGE 0/0/1 of SwitchB functions as the designated port in the CIST.

Run the **display stp interface brief** commands on SwitchD. The displayed information is as follows:

```
<SwitchD> display stp interface XGigabitEthernet 0/0/3 brief
 MSTID      Port                    Role  STP State     Protection
   0        XGigabitEthernet0/0/3    ROOT  FORWARDING      NONE
   1        XGigabitEthernet0/0/3    DESI  FORWARDING      NONE
<SwitchD> display stp interface XGigabitEthernet 0/0/2 brief
 MSTID      Port                    Role  STP State     Protection
   0        XGigabitEthernet0/0/2    ALTE  DISCARDING      NONE
   1        XGigabitEthernet0/0/2    ALTE  DISCARDING      NONE
```

On SwitchD, XGE 0/0/2 functions as the alternate port in the CIST. SwitchD and SwitchC are in different regions; therefore, XGE 0/0/2 of SwitchD also functions as the alternate port in MSTI1.

XGE 0/0/3 of SwitchD is the root port in the CIST. The priority of SwitchD is higher than that of SwitchB in MSTI1; therefore, XGE 0/0/3 also functions as the designated port in MSTI1.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 2 to 20
#
 stp instance 0 priority 0
 stp instance 1 priority 0
 stp pathcost-standard legacy
 stp region-configuration
```

```
 region-name RG1
 instance 1 vlan 1 to 10
 active region-configuration
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
 stp root-protection
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
 stp root-protection
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 2 to 20
#
 stp instance 0 priority 4096
 stp pathcost-standard legacy
 stp region-configuration
 region-name RG2
 instance 1 vlan 1 to 10
 active region-configuration
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
vlan batch 2 to 20
#
stp bpdu-protection
 stp pathcost-standard legacy
 stp region-configuration
 region-name RG1
 instance 1 vlan 1 to 10
 active region-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
 stp edged-port enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
```

```
#
vlan batch 2 to 20
#
 stp instance 1 priority 0
 stp bpdu-protection
 stp pathcost-standard legacy
 stp region-configuration
 region-name RG2
 instance 1 vlan 1 to 10
 active region-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 stp edged-port enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 20
#
Return
```

1.9.2 Example for Configuring MSTP Multi-Process for Layer 2 Single-Access Rings and Layer 2 Multi-Access Rings

MSTP multi-process enables different Layer 2 access rings to transmit different services.

Networking Requirements

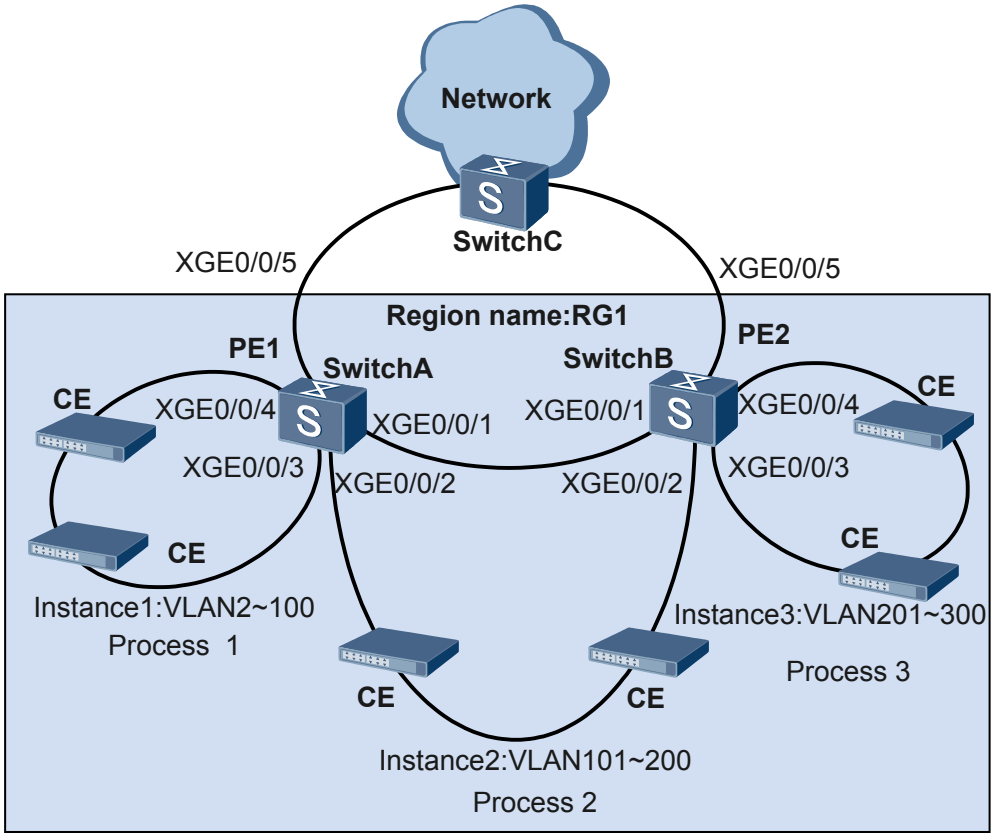
On the network with both Layer 2 single-access rings and multi-access rings deployed, switching devices transmit both Layer 2 and Layer 3 services. To enable different rings to transmit different services, configure MSTP multi-process. Spanning trees of different processes are calculated independently.

As shown in **Figure 1-27**, both Layer 2 single-access rings and dual-access rings are deployed and switches A and B carry both Layer 2 and Layer 3 services. Switches A and B connected to dual-access rings are also connected to a single-access ring.

NOTE

In the ring where MSTP multi-process is configured, you are advised not to block the interface directly connected to the root protection-enabled designated port.

Figure 1-27 Networking for MSTP multi-process for Layer 2 single-access rings and multi-access rings



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic MSTP functions, add devices to MST regions, and create MSTIs.

   NOTE

   - Each ring can belong to only one region.
   - Each CE can join only one ring.

2. Configure multiple MSTP processes, including:

   (1) Create multiple MSTP processes and add interfaces to relevant processes.

   (2) Configure a share-link.

3. Configure MSTP protection functions, including:
   - Configure priorities of MSTP processes and enable root protection.
   - Configure share-link protection.
4. Configure the Layer 2 forwarding function on devices.

Data Preparation

To complete the configuration, you need the following data:

- Name of an MST region and names of MSTIs
- VLAN IDs
- IDs of MSTP processes

Procedure

Step 1 Configure basic MSTP functions, add devices to an MST region, and create MSTIs.

1. Configure MST regions and create MSTIs.

   # Configure an MST region and create MSTIs on Switch A.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchA
   [SwitchA] stp region-configuration
   [SwitchA-mst-region] region-name RG1
   [SwitchA-mst-region] instance 1 vlan 2 to 100
   [SwitchA-mst-region] instance 2 vlan 101 to 200
   [SwitchA-mst-region] instance 3 vlan 201 to 300
   [SwitchA-mst-region] active region-configuration
   [SwitchA-mst-region] quit
   ```

   # Configure an MST region and create MSTIs on Switch B.

   ```
   <Quidway> system-view
   [Quidway] sysname SwitchB
   [SwitchB] stp region-configuration
   [SwitchB-mst-region] region-name RG1
   [SwitchB-mst-region] instance 1 vlan 2 to 100
   [SwitchB-mst-region] instance 2 vlan 101 to 200
   [SwitchB-mst-region] instance 3 vlan 201 to 300
   [SwitchB-mst-region] active region-configuration
   [SwitchB-mst-region] quit
   ```

2. Enable MSTP.

   # Configure Switch A.

   ```
   [SwitchA] stp enable
   ```

   # Configure Switch B.

   ```
   [SwitchB] stp enable
   ```

Step 2 Configure multiple MSTP processes.

1. Create multiple MSTP processes and add interfaces to relevant processes.

   # Create MSTP processes 1 and 2 on Switch A.

   ```
   [SwitchA] stp process 1
   [SwitchA-mst-process-1] quit
   [SwitchA] stp process 2
   [SwitchA-mst-process-2] quit
   ```

   # Create MSTP processes 2 and 3 on Switch B.

   ```
   [SwitchB] stp process 2
   [SwitchB-mst-process-2] quit
   [SwitchB] stp process 3
   [SwitchB-mst-process-3] quit
   ```

   # Add XGE 0/0/3 and XGE 0/0/4 on Switch A to MSTP process 1 and XGE 0/0/2 to MSTP process 2.

   ```
   [SwitchA] interface xgigabitethernet 0/0/4
   [SwitchA-XGigabitEthernet0/0/4] bpdu enable
   [SwitchA-XGigabitEthernet0/0/4] stp binding process 1
   [SwitchA-XGigabitEthernet0/0/4] quit
   [SwitchA] interface xgigabitethernet 0/0/3
   [SwitchA-XGigabitEthernet0/0/3] bpdu enable
   [SwitchA-XGigabitEthernet0/0/3] stp binding process 1
   [SwitchA-XGigabitEthernet0/0/3] quit
   ```

```
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] bpdu enable
[SwitchA-XGigabitEthernet0/0/2] stp binding process 2
[SwitchA-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/3 and XGE 0/0/4 on Switch B to MSTP process 3 and XGE 0/0/2 to MSTP process 2.

```
[SwitchB] interface xgigabitethernet 0/0/4
[SwitchB-XGigabitEthernet0/0/4] bpdu enable
[SwitchB-XGigabitEthernet0/0/4] stp binding process 3
[SwitchB-XGigabitEthernet0/0/4] quit
[SwitchB] interface xgigabitethernet 0/0/3
[SwitchB-XGigabitEthernet0/0/3] bpdu enable
[SwitchB-XGigabitEthernet0/0/3] stp binding process 3
[SwitchB-XGigabitEthernet0/0/3] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] bpdu enable
[SwitchB-XGigabitEthernet0/0/2] stp binding process 2
[SwitchB-XGigabitEthernet0/0/2] quit
```

2. Configure a share-link.

   # Configure Switch A.

```
[SwitchA] interface xgigabitethernet0/0/1
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
[SwitchA-XGigabitEthernet0/0/1] stp binding process 2 link-share
[SwitchA-XGigabitEthernet0/0/1] quit
```

   # Configure Switch B.

```
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] bpdu enable
[SwitchB-XGigabitEthernet0/0/1] stp binding process 2 link-share
[SwitchB-XGigabitEthernet0/0/1] quit
```

3. Enable the MSTP function in MSTP multi-process.

   # Configure Switch A.

```
[SwitchA] stp process 1
[SwitchA-stp-process-1] stp enable
[SwitchA-stp-process-1] quit
[SwitchA] stp process 2
[SwitchA-stp-process-2] stp enable
[SwitchA-stp-process-2] quit
```

   # Configure Switch B.

```
[SwitchB] stp process 3
[SwitchB-stp-process-3] stp enable
[SwitchB-stp-process-3] quit
[SwitchB] stp process 2
[SwitchB-stp-process-2] stp enable
[SwitchB-stp-process-2] quit
```

Step 3 Configure MSTP protection functions.

- Configure priorities of MSTP processes and enable root protection.

  # Configure Switch A.

```
[SwitchA] stp process 1
[SwitchA-stp-process-1] stp instance 0 root primary
[SwitchA-stp-process-1] stp instance 1 root primary
[SwitchA-stp-process-1] quit
[SwitchA] stp process 2
[SwitchA-stp-process-2] stp instance 0 root primary
[SwitchA-stp-process-2] stp instance 2 root primary
[SwitchA-stp-process-2] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp root-protection
[SwitchA-XGigabitEthernet0/0/2] quit
```

  # Configure Switch B.

```
[SwitchB] stp process 3
[SwitchB-stp-process-3] stp instance 0 root primary
[SwitchB-stp-process-3] stp instance 3 root primary
[SwitchB-stp-process-3] quit
[SwitchB] stp process 2
[SwitchB-stp-process-2] stp instance 0 root secondary
[SwitchB-stp-process-2] stp instance 2 root secondary
[SwitchB-stp-process-2] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] stp root-protection
[SwitchB-XGigabitEthernet0/0/2] quit
```

NOTE

- In each ring, the priority of the MSTP process on the downstream CE must be lower than the priority of the MSTP process on the switching device.
- For switches A and B on the dual-access ring, you are recommended to configure them as the primary root bridges of different MSTIs.

- Configure share-link protection.

  # Configure Switch A.

```
[SwitchA] stp process 2
[SwitchA-stp-process-2] stp link-share-protection
[SwitchA-stp-process-2] quit
```

  # Configure Switch B.

```
[SwitchB] stp process 2
[SwitchB-stp-process-2] stp link-share-protection
[SwitchB-stp-process-2] quit
```

Step 4 Create VLANs and add interfaces to VLANs.

Create VLANs 2 to 200 on Switch A. Add XGE 0/0/3 and XGE 0/0/4 to VLANs 2 to 100, and add XGE 0/0/1 and XGE 0/0/2 to VLANs 101 to 200.

```
[SwitchA] vlan batch 2 to 200
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] port link-type  trunk
[SwitchA-XGigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 100
[SwitchA-XGigabitEthernet0/0/3] quit
[SwitchA] interface xgigabitethernet 0/0/4
[SwitchA-XGigabitEthernet0/0/4] port link-type  trunk
[SwitchA-XGigabitEthernet0/0/4] port trunk allow-pass vlan 2 to 100
[SwitchA-XGigabitEthernet0/0/4] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type  trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 101 to 200
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type  trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 101 to 200
[SwitchA-XGigabitEthernet0/0/2] quit
```

Create VLANs 101 to 300 on Switch B. Add XGE 0/0/3 and XGE 0/0/4 to VLANs 201 to 300, and add XGE 0/0/1 and XGE 0/0/2 to VLANs 101 to 200.

```
[SwitchB] vlan batch 101 to 300
[SwitchB] interface xgigabitethernet 0/0/3
[SwitchB-XGigabitEthernet0/0/3] port link-type  trunk
[SwitchB-XGigabitEthernet0/0/3] port trunk allow-pass vlan 201 to 300
[SwitchB-XGigabitEthernet0/0/3] quit
[SwitchB] interface xgigabitethernet 0/0/4
[SwitchB-XGigabitEthernet0/0/4] port link-type  trunk
[SwitchB-XGigabitEthernet0/0/4] port trunk allow-pass vlan 201 to 300
[SwitchB-XGigabitEthernet0/0/4] quit
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type  trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 101 to 200
```

```
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] port link-type  trunk
[SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 101 to 200
[SwitchB-XGigabitEthernet0/0/2] quit
```

Step 5 Verify the configuration.

- Run the **display stp interface brief** command on Switch A, and you can view the following information:

  # XGE 0/0/4 is a designated port in the CIST of MSTP process 1 and in MSTI 1.

```
[SwitchA] display stp process 1 interface GiabitEthernet 0/0/4 brief
 MSTID      Port                  Role  STP State       Protection
   0    XGigabitEthernet0/0/4        DESI  FORWARDING      NONE
   1    XGigabitEthernet0/0/4        DESI  FORWARDING      NONE
```

  # XGE 0/0/2 is a designated port in the CIST of MSTP process 2 and in MSTI 2.

```
[SwitchA] display stp process 2 interface giabitethernet 0/0/2 brief
 MSTID      Port                  Role  STP State       Protection
   0    XGigabitEthernet0/0/2        DESI  FORWARDING      ROOT
   2    XGigabitEthernet0/0/2        DESI  FORWARDING      ROOT
```

- Run the **display stp interface brief** command on Switch B, and you can view the following information:

  # XGE 0/0/4 is a designated port in the CIST of MSTP process 3 and in MSTI 3.

```
[SwitchB] display stp process 3 interface giabitethernet 0/0/4 brief
 MSTID      Port                  Role  STP State       Protection
   0    XGigabitEthernet0/0/4        DESI  FORWARDING      NONE
   3    XGigabitEthernet0/0/4        DESI  FORWARDING      NONE
```

  # XGE 0/0/2 is a designated port in the CIST of MSTP process 2 and in MSTI 2.

```
[SwitchB] display stp process 2 interface giabitethernet 0/0/2 brief
 MSTID      Port                  Role  STP State       Protection
   0    XGigabitEthernet0/0/2        DESI  FORWARDING      ROOT
   2    XGigabitEthernet0/0/2        DESI  FORWARDING      ROOT
```

----End

Configuration Files

Only the MSTP-related configuration files are listed.

- Configuration file of Switch A

```
#
 sysname
SwitchA
#
 vlan batch 2 to
300

#
 stp region-
configuration
  region-name
RG1
  instance 1 vlan 2 to
100
  instance 2 vlan 101 to
200
  instance 3 vlan 201 to
300
  active region-
configuration
#
stp process
```

```
1
 stp instance 0 root
primary
 stp instance 1 root
primary
 stp
enable
stp process
2
 stp instance 0 root
primary
 stp instance 2 root
primary
 stp link-share-
protection
 stp
enable
#
interface
XGigabitEthernet0/0/1
 port link-type  trunk
 port trunk allow-pass vlan 101 to
200
 stp binding process 2 link-share
#
interface
XGigabitEthernet0/0/2
 port link-type  trunk
 port trunk allow-pass vlan 101 to
200
 stp binding process
2
 stp root-
protection
#
interface XGigabitEthernet0/0/3
 port link-type  trunk
 port trunk allow-pass vlan 2 to
100
 stp binding process
1
#
interface XGigabitEthernet0/0/4
 port link-type  trunk
 port trunk allow-pass vlan 2 to
100
 stp binding process 1
#
return
```

- Configuration file of Switch B

```
#
 sysname
SwitchB
#
 vlan batch 2 to
300
#
 stp region-
configuration
  region-name
RG1
  instance 1 vlan 2 to
100
  instance 2 vlan 101 to
200
  instance 3 vlan 201 to
300
  active region-
configuration
```

```
#
stp process
2
 stp instance 0 root
secondary
 stp instance 2 root
secondary
 stp link-share-
protection
 stp
enable
stp process
3
 stp instance 0 root
primary
 stp instance 3 root
primary
 stp
enable
#
interface XGigabitEthernet0/0/1
 port link-type  trunk
 port trunk allow-pass vlan 101 to
200
 stp binding process 2 link-
share
#
interface XGigabitEthernet0/0/2
 port link-type  trunk
 port trunk allow-pass vlan 101 to
200
 stp binding process
2
 stp root-
protection
#
interface XGigabitEthernet0/0/3
 port link-type  trunk
 port trunk allow-pass vlan 201 to
300
 stp binding process
3
#
interface XGigabitEthernet0/0/4
 port link-type  trunk
 port trunk allow-pass vlan 201 to
300
 stp binding process
3
#
return
```

1.10 SEP Configuration

As a link layer protocol dedicated to Ethernet rings, SEP blocks redundant links on a network to prevent logical loops.

1.10.1 Example for Configuring SEP on a Closed Ring Network

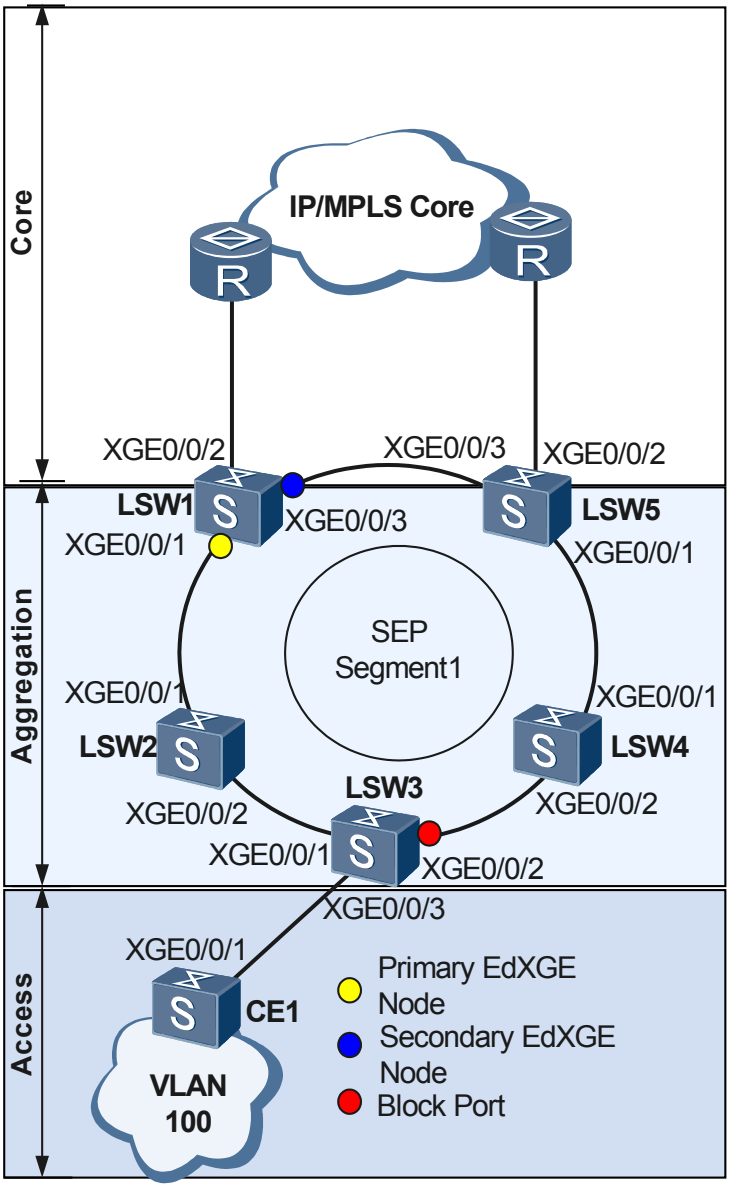
In the closed ring networking, CE1 is dual homed to a Layer 2 network through multiple Layer 2 switching devices. The two edge devices connected to the upper-layer Layer 2 network are directly connected to each other. The closed ring network is deployed at the aggregation layer to implement Layer 2 transparent transmission of unicast and multicast packets. SEP runs at the aggregation layer to implement link redundancy.

Networking Requirements

Generally, redundant links are used to connect an Ethernet switching network to an upper-layer network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, the communication quality deteriorates, and communication services may even be interrupted. SEP can be deployed on the ring network to block redundant links and unblock them if a link fault occurs.

As shown in **Figure 1-28**, Layer 2 switching devices LSW1 to LSW5 form a ring network, which is connected to the core network. SEP runs at the aggregation layer. When the ring network is normal, SEP blocks the redundant Ethernet links. When a link on the ring fails, SEP can quickly restore communication between the nodes on the ring.

Figure 1-28 Networking diagram of a closed ring SEP network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
   (1) Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.
   (2) Add all devices on the ring to SEP segment 1, and configure the roles of XGE0/0/1 and XGE0/0/3 of LSW1 in SEP segment 1.
   (3) On the device where the primary edge port is located, specify that the port with the highest priority will be blocked.
   (4) Set priorities of the ports in the SEP segment.

   Set the highest priority for XGE0/0/2 of LSW3 and retain the default priority of the other ports so that XGE0/0/2 of LSW3 will be blocked.
   (5) Configure delayed preemption on the device where the primary edge port is located.
2. Configure the Layer 2 forwarding function on CE1 and LSW1 to LSW5.

Data Preparation

To complete the configuration, you need the following data:

- SEP segment ID
- Control VLAN of the SEP segment
- Port roles in the SEP segment
- Preemption mode
- Method of selecting the port to block
- Priorities of the ports in the SEP segment

Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.

   # Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

   # Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

   # Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
```

```
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

Configure LSW4.

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] protected-instance all
[LSW4-sep-segment1] quit
```

Configure LSW5.

```
<Quidway> system-view
[Quidway] sysname LSW5
[LSW5] sep segment 1
[LSW5-sep-segment1] control-vlan 10
[LSW5-sep-segment1] protected-instance all
[LSW5-sep-segment1] quit
```

NOTE

- The control VLAN must be a VLAN that has not been created or used, but the configuration file automatically displays the command for creating the VLAN.
- Each SEP segment must be configured with a control VLAN. After an interface is added to the SEP segment configured with a control VLAN, the interface is added to the control VLAN automatically. The configuration file displays **port hybrid tagged vlan** under this interface.

2. Add all devices on the ring to SEP segment 1 and configure port roles on the devices.

NOTE

By default, STP is enabled on a Layer 2 interface. Before adding an interface to the SEP segment, disable STP on the interface.

On LSW1, configure XGE0/0/1 as the primary edge port and XGE0/0/3 as the secondary edge port.

```
[LSW1] interface xgigabitethernet 0/0/1
[LSW1-XGigabitEthernet0/0/1] stp disable
[LSW1-XGigabitEthernet0/0/1] sep segment 1 edge primary
[LSW1-XGigabitEthernet0/0/1] quit
[LSW1] interface xgigabitethernet 0/0/3
[LSW1-XGigabitEthernet0/0/3] stp disable
[LSW1-XGigabitEthernet0/0/3] sep segment 1 edge secondary
[LSW1-XGigabitEthernet0/0/3] quit
```

Configure LSW2.

```
[LSW2] interface xgigabitethernet 0/0/1
[LSW2-XGigabitEthernet0/0/1] stp disable
[LSW2-XGigabitEthernet0/0/1] sep segment 1
[LSW2-XGigabitEthernet0/0/1] quit
[LSW2] interface xgigabitethernet 0/0/2
[LSW2-XGigabitEthernet0/0/2] stp disable
[LSW2-XGigabitEthernet0/0/2] sep segment 1
[LSW2-XGigabitEthernet0/0/2] quit
```

Configure LSW3.

```
[LSW3] interface xgigabitethernet 0/0/1
[LSW3-XGigabitEthernet0/0/1] stp disable
[LSW3-XGigabitEthernet0/0/1] sep segment 1
[LSW3-XGigabitEthernet0/0/1] quit
[LSW3] interface xgigabitethernet 0/0/2
[LSW3-XGigabitEthernet0/0/2] stp disable
[LSW3-XGigabitEthernet0/0/2] sep segment 1
[LSW3-XGigabitEthernet0/0/2] quit
```

Configure LSW4.

```
[LSW4] interface xgigabitethernet 0/0/1
[LSW4-XGigabitEthernet0/0/1] stp disable
[LSW4-XGigabitEthernet0/0/1] sep segment 1
[LSW4-XGigabitEthernet0/0/1] quit
[LSW4] interface xgigabitethernet 0/0/2
[LSW4-XGigabitEthernet0/0/2] stp disable
```

```
[LSW4-XGigabitEthernet0/0/2] sep segment 1
[LSW4-XGigabitEthernet0/0/2] quit
```

Configure LSW5.

```
[LSW5] interface xgigabitethernet 0/0/1
[LSW5-XGigabitEthernet0/0/1] stp disable
[LSW5-XGigabitEthernet0/0/1] sep segment 1
[LSW5-XGigabitEthernet0/0/1] quit
[LSW5] interface xgigabitethernet 0/0/3
[LSW5-XGigabitEthernet0/0/3] stp disable
[LSW5-XGigabitEthernet0/0/3] sep segment 1
[LSW5-XGigabitEthernet0/0/3] quit
```

3. Specify a port to block.

   # On LSW1 where the primary edge port is located, specify that the port with the highest priority is blocked.

   ```
   [LSW1] sep segment 1
   [LSW1-sep-segment1] block port optimal
   ```

4. Set the priority of XGE0/0/2 on LSW3.

   ```
   [LSW3] interface xgigabitethernet 0/0/2
   [LSW3-XGigabitEthernet0/0/2] sep segment 1 priority 128
   [LSW3-XGigabitEthernet0/0/2] quit
   ```

5. Configure the preemption mode.

   # Configure the delayed preemption mode on LSW1.

   ```
   [LSW1-sep-segment1] preempt delay 30
   [LSW1-sep-segment1] quit
   ```

   NOTE

   - You must set the preemption delay when delayed preemption is adopted because there is no default delay time.
   - After all the faulty ports recover, the edge ports no longer receive fault notification packets. If the primary edge port does not receive any fault notification packet, it starts the delay timer. When the delay timer expires, nodes in the SEP segment start blocked port preemption.

     To implement delayed preemption in this example, you need to simulate a port fault and then rectify the fault. For example:

     Run the **shutdown** command on XGE0/0/2 of LSW2 to simulate a port fault, and then run the **undo shutdown** command on XGE0/0/2 to rectify the fault.

Step 2 Configure the Layer 2 forwarding function on CE1 and LSW1 to LSW5.

For details about the configuration, see the configuration files.

Step 3 Verify the configuration.

- Run the **shutdown** command on XGE0/0/1 of LSW3 to simulate a port fault, and then run the display sep interface command on LSW3 to check whether XGE0/0/2 of LSW3 switches from the Discarding state to the Forwarding state.

  ```
  <LSW3> display sep interface xgigabitethernet 0/0/2
  SEP segment 1
  ------------------------------------------------------------------
  Interface           Port Role     Neighbor Status     Port Status
  ------------------------------------------------------------------
  XGE0/0/2             common        up                  forwarding
  ```

----End

Configuration Files

- Configuration file of LSW1

  ```
  #
   sysname LSW1
  ```

```
#
 vlan batch 10 100 200
#
sep segment 1
 control-vlan 10
 block port optimal
 preempt delay 30
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1 edge primary
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1 edge secondary
#
return
```

- Configuration file of LSW2

```
#
 sysname LSW2
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

- Configuration file of LSW3

```
#
 sysname LSW3
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
 sep segment 1 priority 128
#
interface XGigabitEthernet0/0/3
```

```
 port hybrid tagged vlan 100
#
return
```

- Configuration file of LSW4

```
#
 sysname LSW4
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

- Configuration file of LSW5

```
#
 sysname LSW5
#
 vlan batch 10 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
return
```

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
return
```

1.10.2 Example for Configuring SEP on a Multi-ring Network

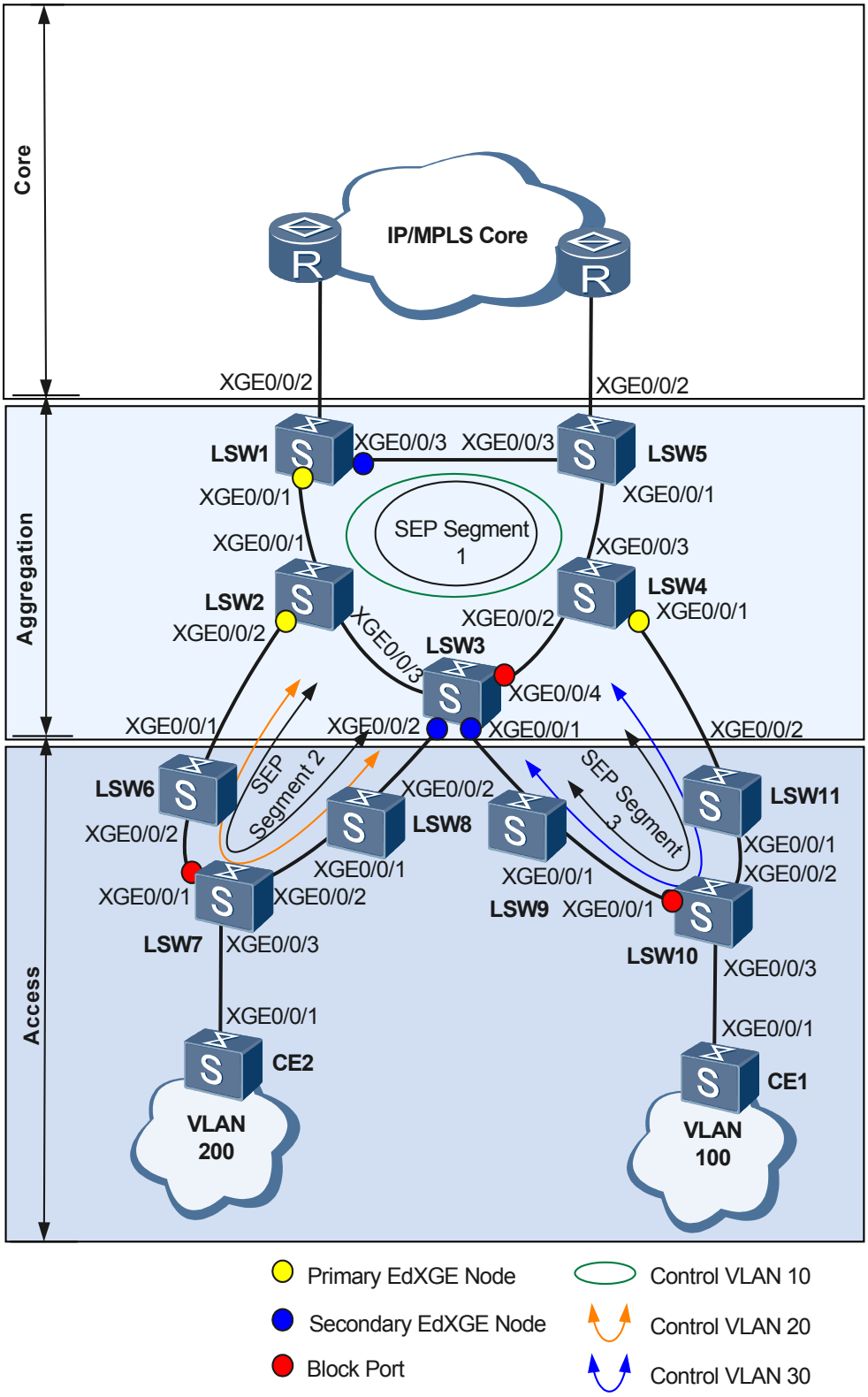
In multi-ring networking, multiple rings consisting of Layer 2 switching devices are deployed at the access layer and aggregation layer. SEP runs at the access layer and aggregation layer to implement link redundancy.

Networking Requirements

Generally, redundant links are used to connect an Ethernet switching network to an upper-layer network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, the communication quality deteriorates, and communication services may even be interrupted. SEP can be deployed on the ring network to block redundant links and unblock them if a link fault occurs.

As shown in **Figure 1-29**, multiple Layer 2 switching devices form ring networks at the access layer and aggregation layer. The ring network at the aggregation layer is connected to the core layer. SEP runs at the access layer and aggregation layer. When the ring network is normal, SEP blocks the redundant Ethernet links. When a link on the ring fails, SEP can quickly restore communication between nodes on the ring.

Figure 1-29 Networking diagram of a multi-ring SEP network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
   (1) Configure SEP segments 1 to 3 and configure VLAN 10, VLAN 20, and VLAN 30 as their control VLANs.
   - Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.
   - Configure SEP segment 2 on LSW2, LSW3, and LSW6 to LSW8, and configure VLAN 20 as the control VLAN of SEP segment 2.
   - Configure SEP segment 3 on LSW3, LSW4, and LSW9 to LSW11, and configure VLAN 30 as the control VLAN of SEP segment 3.

   (2) Add devices on the rings to the SEP segments and configure port roles on the edge devices of the SEP segments.
   - On LSW1 to LSW5, add the interfaces on the ring at the access layer to SEP segment 1. Configure the roles of XGE0/0/1 and XGE0/0/3 of LSW1 in SEP segment 1.
   - Add XGE0/0/2 of LSW2, XGE0/0/1 and XGE0/0/2 of LSW6 to LSW8, and XGE0/0/2 of LSW3 to SEP segment 2. Configure the roles of XGE0/0/2 of LSW2 and XGE0/0/2 of LSW3 in SEP segment 2.
   - Add XGE0/0/1 of LSW3, XGE0/0/1 and XGE0/0/2 of LSW9 to LSW11, and XGE0/0/1 of LSW4 to SEP segment 3. Configure the roles of XGE0/0/1 of LSW2 and XGE0/0/1 of LSW3 in SEP segment 3.

   (3) Specify the port to block on the device where the primary edge port is located.
   - In SEP segment 1, specify that the port with the highest priority will be blocked.
   - In SEP segment 2, specify the device name and port name to block the specified port.
   - In SEP segment 3, specify that the blocked port be selected according to the configured hop counts of ports.

   (4) Configure the preemption mode on the device where the primary edge port is located.

   Configure delayed preemption in SEP segment 1 and manual preemption in SEP segment 2 and SEP segment 3.

   (5) Configure the topology change notification function on the edge devices between SEP segments, namely, LSW2, LSW3, and LSW4.
2. Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW11.

Data Preparation

To complete the configuration, you need the following data:

- SEP segment ID
- Control VLAN of the SEP segment
- Port roles in the SEP segment
- Preemption mode
- Method of selecting the port to block
- Priorities of the ports in the SEP segment

Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segments 1 to 3 and configure VLAN 10, VLAN 20, and VLAN 30 as their control VLANs, as shown in **Figure 1-29**.

   # Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

   # Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
[LSW2] sep segment 2
[LSW2-sep-segment2] control-vlan 20
[LSW2-sep-segment2] protected-instance all
[LSW2-sep-segment2] quit
```

   # Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
[LSW3] sep segment 2
[LSW3-sep-segment2] control-vlan 20
[LSW3-sep-segment2] protected-instance all
[LSW3-sep-segment2] quit
[LSW3] sep segment 3
[LSW3-sep-segment3] control-vlan 30
[LSW3-sep-segment3] protected-instance all
[LSW3-sep-segment3] quit
```

   # Configure LSW4.

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] protected-instance all
[LSW4-sep-segment1] quit
[LSW4] sep segment 3
[LSW4-sep-segment3] control-vlan 30
[LSW4-sep-segment3] protected-instance all
[LSW4-sep-segment3] quit
```

   # Configure LSW5.

```
<Quidway> system-view
[Quidway] sysname LSW5
[LSW5] sep segment 1
[LSW5-sep-segment1] control-vlan 10
[LSW5-sep-segment1] protected-instance all
[LSW5-sep-segment1] quit
```

   # Configure LSW6 to LSW11.

   The configurations of LSW6 to LSW11 are similar to the configurations of LSW1 to LSW5 except for the control VLANs of different SEP segments.

   For details about the configuration, see the configuration files.

NOTE

- The control VLAN must be a VLAN that has not been created or used, but the configuration file automatically displays the command for creating the VLAN.
- Each SEP segment must be configured with a control VLAN. After an interface is added to the SEP segment configured with a control VLAN, the interface is added to the control VLAN automatically. The configuration file displays **port hybrid tagged vlan** under this interface.

2. Add devices on the rings to the SEP segments and configure port roles according to **Figure 1-29**.

NOTE

By default, STP is enabled on a Layer 2 interface. Before adding an interface to the SEP segment, disable STP on the interface.

On LSW1, configure XGE0/0/1 as the primary edge port and XGE0/0/3 as the secondary edge port.

```
[LSW1] interface xgigabitethernet 0/0/1
[LSW1-XGigabitEthernet0/0/1] stp disable
[LSW1-XGigabitEthernet0/0/1] sep segment 1 edge primary
[LSW1-XGigabitEthernet0/0/1] quit
[LSW1] interface xgigabitethernet 0/0/3
[LSW1-XGigabitEthernet0/0/3] stp disable
[LSW1-XGigabitEthernet0/0/3] sep segment 1 edge secondary
[LSW1-XGigabitEthernet0/0/3] quit
```

Configure LSW2.

```
[LSW2] interface xgigabitethernet 0/0/1
[LSW2-XGigabitEthernet0/0/1] stp disable
[LSW2-XGigabitEthernet0/0/1] sep segment 1
[LSW2-XGigabitEthernet0/0/1] quit
[LSW2] interface xgigabitethernet 0/0/3
[LSW2-XGigabitEthernet0/0/3] stp disable
[LSW2-XGigabitEthernet0/0/3] sep segment 1
[LSW2-XGigabitEthernet0/0/3] quit
[LSW2] interface xgigabitethernet 0/0/2
[LSW2-XGigabitEthernet0/0/2] stp disable
[LSW2-XGigabitEthernet0/0/2] sep segment 2 edge primary
[LSW2-XGigabitEthernet0/0/2] quit
```

Configure LSW3.

```
[LSW3] interface xgigabitethernet 0/0/3
[LSW3-XGigabitEthernet0/0/3] stp disable
[LSW3-XGigabitEthernet0/0/3] sep segment 1
[LSW3-XGigabitEthernet0/0/3] quit
[LSW3] interface xgigabitethernet 0/0/4
[LSW3-XGigabitEthernet0/0/4] stp disable
[LSW3-XGigabitEthernet0/0/4] sep segment 1
[LSW3-XGigabitEthernet0/0/4] quit
[LSW3] interface xgigabitethernet 0/0/2
[LSW3-XGigabitEthernet0/0/2] stp disable
[LSW3-XGigabitEthernet0/0/2] sep segment 2 edge secondary
[LSW3-XGigabitEthernet0/0/2] quit
[LSW3] interface xgigabitethernet 0/0/1
[LSW3-XGigabitEthernet0/0/1] stp disable
[LSW3-XGigabitEthernet0/0/1] sep segment 3 edge secondary
[LSW3-XGigabitEthernet0/0/1] quit
```

Configure LSW4.

```
[LSW4] interface xgigabitethernet 0/0/2
[LSW4-XGigabitEthernet0/0/2] stp disable
[LSW4-XGigabitEthernet0/0/2] sep segment 1
[LSW4-XGigabitEthernet0/0/2] quit
[LSW4] interface xgigabitethernet 0/0/3
[LSW4-XGigabitEthernet0/0/3] stp disable
[LSW4-XGigabitEthernet0/0/3] sep segment 1
[LSW4-XGigabitEthernet0/0/3] quit
```

```
[LSW4] interface xgigabitethernet 0/0/1
[LSW4-XGigabitEthernet0/0/1] stp disable
[LSW4-XGigabitEthernet0/0/1] sep segment 3 edge primary
[LSW4-XGigabitEthernet0/0/1] quit
```

Configure LSW5.

```
[LSW5] interface xgigabitethernet 0/0/1
[LSW5-XGigabitEthernet0/0/1] stp disable
[LSW5-XGigabitEthernet0/0/1] sep segment 1
[LSW5-XGigabitEthernet0/0/1] quit
[LSW5] interface xgigabitethernet 0/0/3
[LSW5-XGigabitEthernet0/0/3] stp disable
[LSW5-XGigabitEthernet0/0/3] sep segment 1
[LSW5-XGigabitEthernet0/0/3] quit
```

Configure LSW6 to LSW11.

The configurations of LSW6 to LSW11 are similar to the configurations of LSW1 to LSW5 except for the port roles.

For details about the configuration, see the configuration files.

3. Specify the port to block.

   # On LSW1 where the primary edge port of SEP segment 1 is located, specify that the port with the highest priority be blocked.

   ```
   [LSW1] sep segment 1
   [LSW1-sep-segment1] block port optimal
   [LSW1-sep-segment1] quit
   ```

   # On LSW3, set the priority of XGE0/0/4 to 128, which is the highest priority among the ports so that XGE0/0/4 will be blocked.

   ```
   [LSW3] interface xgigabitethernet 0/0/4
   [LSW3-XGigabitEthernet0/0/4] sep segment 1 priority 128
   [LSW3-XGigabitEthernet0/0/4] quit
   ```

   Use the default priority for the other ports in SEP segment 1.

   # On LSW2 where the primary edge port of SPE segment 2 is located, specify the device name and port name so that the specified port will be blocked.

   Before specifying the port to block, you can use the **display sep topology** command to view the current topology information and obtain information about all the ports in the topology. Then you can select the device name and port name.

   ```
   [LSW2] sep segment 2
   [LSW2-sep-segment2] block port sysname LSW7 interface xgigabitethernet 0/0/1
   [LSW2-sep-segment2] quit
   ```

   # On LSW4 where the primary edge port of SEP segment 3 is located, specify that the blocked port be selected according to the configured hop counts of ports.

   ```
   [LSW4] sep segment 3
   [LSW4-sep-segment3] block port hop 5
   [LSW4-sep-segment3] quit
   ```

   NOTE

   SEP sets the hop count of the primary edge port to 1 and the hop count of the secondary edge port to 2. Hop counts of other ports increase at a step of 1 in the downstream direction of the primary port.

4. Configure the preemption mode.

   # Configure the delayed preemption mode on LSW1.

   ```
   [LSW1] sep segment 1
   [LSW1-sep-segment1] preempt delay 30
   ```

NOTE

- You must set the preemption delay when delayed preemption is adopted because there is no default delay time.
- After all the faulty ports recover, the edge ports no longer receive fault notification packets. If the primary edge port does not receive any fault notification packet, it starts the delay timer. When the delay timer expires, nodes in the SEP segment start blocked port preemption.

  To implement delayed preemption in this example, you need to simulate a port fault and then rectify the fault. For example:

  Run the **shutdown** command on XGE0/0/2 of LSW2 to simulate a port fault, and then run the **undo shutdown** command on XGE0/0/2 to rectify the fault.

Configure the manual preemption mode on LSW2.

```
[LSW2] sep segment 2
[LSW2-sep-segment2] preempt manual
```

Configure the manual preemption mode on LSW4.

```
[LSW4] sep segment 3
[LSW4-sep-segment3] preempt manual
```

5. Configure the topology change notification function.

   # Configure SEP segment 2 to notify SEP segment 1 of topology changes.

   # Configure LSW2.

```
[LSW2] sep segment 2
[LSW2-sep-segment2] tc-notify segment 1
[LSW2-sep-segment2] quit
```

   # Configure LSW3.

```
[LSW3] sep segment 2
[LSW3-sep-segment2] tc-notify segment 1
[LSW3-sep-segment2] quit
```

   # Configure SEP segment 3 to notify SEP segment 1 of topology changes.

   # Configure LSW3.

```
[LSW3] sep segment 3
[LSW3-sep-segment3] tc-notify segment 1
[LSW3-sep-segment3] quit
```

   # Configure LSW4.

```
[LSW4] sep segment 3
[LSW4-sep-segment3] tc-notify segment 1
[LSW4-sep-segment3] quit
```

   NOTE

   The topology change notification function is configured on edge devices between SEP segments so that the upper-layer network can be notified of topology changes on the lower-layer network.

Step 2 Configure the Layer 2 forwarding function on the CEs and LSW1 to LSW11.

For details about the configuration, see the configuration files.

Step 3 Verify the configuration.

After completing the preceding configurations, do as follows to verify the configuration. LSW1 is taken as an example.

- Run the **shutdown** command on XGE0/0/1 of LSW2 to simulate a port fault, and then run the display sep interface command on LSW3 to check whether XGE0/0/4 of LSW3 switches from the Discarding state to the Forwarding state.

```
<LSW3> display sep interface xgigabitethernet 0/0/4
SEP segment 1
------------------------------------------------------------------
```

```
Interface           Port Role     Neighbor Status     Port Status
--------------------------------------------------------------------
XGE0/0/4             common        up                  forwarding
```

----End

Configuration Files

- Configuration file of LSW1

```
#
 sysname LSW1
#
 vlan batch 10 100 200 300
#
sep segment 1
 control-vlan 10
 block port optimal
 preempt delay 30
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1 edge primary
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid tagged vlan 100 200
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200 300
 stp disable
 sep segment 1 edge secondary
#
return
```

- Configuration file of LSW2

```
#
 sysname LSW2
#
 vlan batch 10 20 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
sep segment 2
 control-vlan 20
 block port sysname LSW7 interface XGigabitEthernet0/0/1
 tc-notify segment 1
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2 edge primary
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
return
```

- Configuration file of LSW3

```
#
 sysname LSW3
#
 vlan batch 10 20 30 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
sep segment 2
 control-vlan 20
 tc-notify segment 1
 protected-instance 0 to 48
sep segment 3
 control-vlan 30
 tc-notify segment 1
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3 edge secondary
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2 edge secondary
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/4
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
 sep segment 1 priority 128
#
return
```

- Configuration file of LSW4

```
#
 sysname LSW4
#
 vlan batch 10 30 100 200
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
sep segment 2
 control-vlan 30
 protected-instance 0 to 48
sep segment 3
 control-vlan 30
 block port hop 5
 tc-notify segment 1
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3 edge primary
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
```

```
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
return
```

- Configuration file of LSW5

```
#
 sysname LSW5
#
 vlan batch 10 100 200 300
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100 200
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid tagged vlan 100 200
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 10 100 200 300
 stp disable
 sep segment 1
#
return
```

- Configuration file of LSW6

```
#
 sysname LSW6
#
 vlan batch 20 200
#
sep segment 2
 control-vlan 20
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
return
```

- Configuration file of LSW7

```
#
 sysname LSW7
#
 vlan batch 20 200
#
sep segment 2
 control-vlan 20
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
```

```
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 200
#
return
```

- Configuration file of LSW8

```
#
 sysname LSW8
#
 vlan batch 20 200
#
sep segment 2
 control-vlan 20
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 200
 stp disable
 sep segment 2
#
return
```

- Configuration file of LSW9

```
#
 sysname LSW9
#
 vlan batch 30 100
#
sep segment 3
 control-vlan 30
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
return
```

- Configuration file of LSW10

```
#
 sysname LSW10
#
 vlan batch 30 100
#
sep segment 3
 control-vlan 30
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
```

```
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- Configuration file of LSW11

```
#
 sysname LSW11
#
 vlan batch 30 100
#
sep segment 3
 control-vlan 30
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 30 100
 stp disable
 sep segment 3
#
return
```

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
return
```

- Configuration file of CE2

```
#
 sysname CE2
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 200
#
return
```

1.10.3 Example for Configuring SEP on a Hybrid-ring Network

In the networking of this configuration example, the two devices where the access layer and the aggregation layer are intersected do not support SEP. You can configure SEP at the access layer to implement redundancy protection switching and configure the function of advertising topology changes on an edge device in a SEP segment. This helps an upper-layer network to detect topology changes of a lower-layer network in time.

Networking Requirements

Generally, redundant links are used to connect an Ethernet switching network to an upper-layer network to provide link backup and enhance network reliability. The use of redundant links,

however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, the communication quality deteriorates, and communication services may even be interrupted. SEP can be deployed on the ring network to block redundant links and unblock them if a link fault occurs.

NOTE

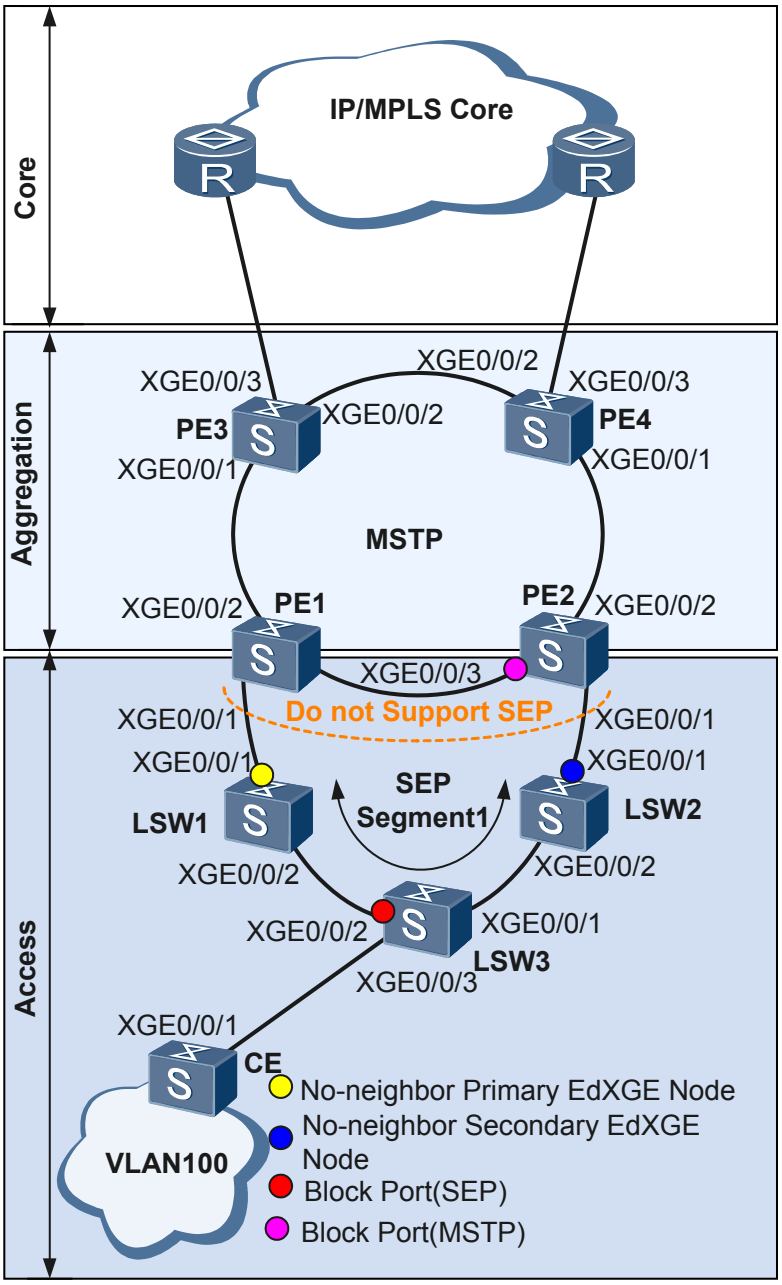
In this example, devices at the aggregation layer run the MSTP protocol.

As shown in **Figure 1-30**, multiple Layer 2 switching devices form a ring at the access layer, and multiple Layer 3 devices form a ring at the aggregation layer, which is connected to the core layer. In this case, SEP needs to run at the access layer to implement the following functions:

- When there is no faulty link on the ring network, SEP helps to eliminate loops.
- When a link fault occurs on the ring network, SEP helps to rapidly restore the communication between nodes.
- The function of advertising topology changes should be configured on an edge device in a SEP segment. This helps an upper-layer network to detect topology changes of a lower-layer network in time.

After receiving a message indicating topology changes of a lower-layer network, a device on an upper-layer network sends TC packets locally to instruct the other devices to clear associated MAC addresses and relearn MAC addresses after the topology of the lower-layer network changes. This ensures nonstop traffic forwarding.

Figure 1-30 Networking diagram of a hybrid-ring SEP network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.

   (1) Configure SEP segment 1 on LSW1 to LSW3 and configure VLAN 10 as the control VLAN of SEP segment 1.

   (2) Add LSW1 to LSW3 to SEP segment 1 and configure port roles on the edge devices of the SEP segment, namely, LSW1 and LSW2.

NOTE

PE1 and PE2 do not support the SEP protocol; therefore, the ports of LSW1 and LSW2 connected to the PEs must be no-neighbor edge ports.

(3) On the device where the no-neighbor primary edge port is located, specify the port in the middle of the SEP segment as the port to block.

(4) Configure manual preemption.

(5) Configure the topology change notification function so that the upper-layer network running MSTP can be notified of topology changes in the SEP segment.

2. Configure basic MSTP functions.

(1) Add PE1 to PE4 to an MST region RG1.

(2) Create VLANs on PE1 to PE4 and add interfaces on the STP ring to the VLANs.

(3) Configure PE3 as the root bridge and PE4 as the backup root bridge.

3. Configure the Layer 2 forwarding function on CE1 and LSW1 to LSW3.

Data Preparation

To complete the configuration, you need the following data:

- SEP segment ID
- Control VLAN of the SEP segment
- Port roles in the SEP segment
- Preemption mode
- Method of selecting the port to block
- MST region name, MSTI ID, and priorities of the PEs in the region

Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

NOTE

- The control VLAN must be a VLAN that has not been created or used, but the configuration file automatically displays the command for creating the VLAN.
- Each SEP segment must be configured with a control VLAN. After an interface is added to the SEP segment configured with a control VLAN, the interface is added to the control VLAN automatically. The configuration file displays **port hybrid tagged vlan** under this interface.

2. Add LSW1 to LSW3 to SEP segment 1 and configure port roles.

   # Configure LSW1.

```
[LSW1] interface xgigabitethernet 0/0/1
[LSW1-XGigabitEthernet0/0/1] sep segment 1 edge no-neighbor primary
[LSW1-XGigabitEthernet0/0/1] quit
[LSW1] interface xgigabitethernet 0/0/2
[LSW1-XGigabitEthernet0/0/2] stp disable
[LSW1-XGigabitEthernet0/0/2] sep segment 1
[LSW1-XGigabitEthernet0/0/2] quit
```

   # Configure LSW2.

```
[LSW2] interface xgigabitethernet 0/0/1
[LSW2-XGigabitEthernet0/0/1] sep segment 1 edge no-neighbor secondary
[LSW2-XGigabitEthernet0/0/1] quit
[LSW2] interface xgigabitethernet 0/0/2
[LSW2-XGigabitEthernet0/0/2] stp disable
[LSW2-XGigabitEthernet0/0/2] sep segment 1
[LSW2-XGigabitEthernet0/0/2] quit
```

   # Configure LSW3.

```
[LSW3] interface xgigabitethernet 0/0/1
[LSW3-XGigabitEthernet0/0/1] stp disable
[LSW3-XGigabitEthernet0/0/1] sep segment 1
[LSW3-XGigabitEthernet0/0/1] quit
[LSW3] interface xgigabitethernet 0/0/2
[LSW3-XGigabitEthernet0/0/2] stp disable
[LSW3-XGigabitEthernet0/0/2] sep segment 1
[LSW3-XGigabitEthernet0/0/2] quit
```

3. Specify the port to block.

   # On LSW1 where the no-neighbor primary edge port of SEP segment 1 is located, specify the port in the middle of the SEP segment as the port to block.

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port middle
```

4. Configure the preemption mode.

   # Configure the manual preemption mode on LSW1.

```
[LSW1-sep-segment1] preempt maunal
```

5. Configure the topology change notification function.

   # Configure SEP segment 1 to notify the MSTP network of topology changes.

   # Configure LSW1.

```
[LSW1-sep-segment1] tc-notify stp
[LSW1-sep-segment1] quit
```

   # Configure LSW2.

```
[LSW2] sep segment 1
[LSW2-sep-segment1] tc-notify stp
[LSW2-sep-segment1] quit
```

After completing the preceding configurations, do as follows to verify the configuration. LSW1 is taken as an example.

- Run the display sep topology command on LSW1 to view detailed topology information of the SEP segment.

The topology information shows that XGE0/0/2 of LSW3 is in Discarding state, and the other ports are in Forwarding state.

```
<LSW1> display sep topology
SEP segment 1
------------------------------------------------------------------
System Name      Port Name           Port Role       Port Status
------------------------------------------------------------------
LSW1             XGE0/0/1             *primary        forwarding
LSW1             XGE0/0/2             common          forwarding
LSW3             XGE0/0/1             common          forwarding
LSW3             XGE0/0/2             common          discarding
LSW2             XGE0/0/1             common          forwarding
LSW2             XGE0/0/2             *secondary      forwarding
```

Step 2 Configure basic MSTP functions.

1. Configure an MST region

   # Configure PE1.

   ```
   <Quidway> system-view
   [Quidway] sysname PE1
   [PE1] stp region-configuration
   [PE1-mst-region] region-name RG1
   [PE1-mst-region] active region-configuration
   [PE1-mst-region] quit
   ```

   # Configure PE2.

   ```
   <Quidway> system-view
   [Quidway] sysname PE2
   [PE2] stp region-configuration
   [PE2-mst-region] region-name RG1
   [PE2-mst-region] active region-configuration
   [PE2-mst-region] quit
   ```

   # Configure PE3.

   ```
   <Quidway> system-view
   [Quidway] sysname PE3
   [PE3] stp region-configuration
   [PE3-mst-region] region-name RG1
   [PE3-mst-region] active region-configuration
   [PE3-mst-region] quit
   ```

   # Configure PE4.

   ```
   <Quidway> system-view
   [Quidway] sysname PE4
   [PE4] stp region-configuration
   [PE4-mst-region] region-name RG1
   [PE4-mst-region] active region-configuration
   [PE4-mst-region] quit
   ```

2. Create VLANs and add interfaces to VLANs.

   # On PE1, create VLAN 100 and add XGE0/0/1, XGE0/0/2, and XGE0/0/3 to VLAN 100.

   ```
   [PE1] vlan 100
   [PE1-vlan100] quit
   [PE1] interface xgigabitethernet 0/0/1
   [PE1-XGigabitEthernet0/0/1] port hybrid tagged vlan 100
   [PE1-XGigabitEthernet0/0/1] quit
   [PE1] interface xgigabitethernet 0/0/2
   [PE1-XGigabitEthernet0/0/2] port hybrid tagged vlan 100
   [PE1-XGigabitEthernet0/0/2] quit
   [PE1] interface xgigabitethernet 0/0/3
   [PE1-XGigabitEthernet0/0/3] port hybrid tagged vlan 100
   [PE1-XGigabitEthernet0/0/3] quit
   ```

   # On PE2, PE3, and PE4, create VLAN 100 and add XGE0/0/1, XGE0/0/2, and XGE0/0/3 to VLAN 100.

The configurations of PE2, PE3, and PE3 are similar to the configuration of PE1, and are not mentioned here. For details about the configuration, see the configuration files.

3. Enable MSTP.

   # Configure PE1.

   ```
   [PE1] stp enable
   ```

   # Configure PE2.

   ```
   [PE2] stp enable
   ```

   # Configure PE3.

   ```
   [PE3] stp enable
   ```

   # Configure PE4.

   ```
   [PE4] stp enable
   ```

4. Configure PE3 as the root bridge and PE4 as the backup root bridge.

   # Set the priority of PE3 to 0 in MSTI0 to ensure that PE3 functions as the root bridge.

   ```
   [PE3] stp instance 0 priority 0
   [PE3] stp root primary
   ```

   # Set the priority of PE4 to 4096 in MSTI0 to ensure that PE4 functions as the backup root bridge.

   ```
   [PE4] stp instance 0 priority 4096
   [PE4] stp root secondary
   ```

After the configuration, run the **display stp brief** command on PE2 to check whether XGE0/0/3 is blocked.

```
<PE4> display stp brief
MSTID  Port                        Role  STP State     Protection
   0    XGigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    XGigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0    XGigabitEthernet0/0/3        ALTE  DISCARDING      NONE
```

Step 3 Configure the Layer 2 forwarding function on the CE and LSW1 to LSW3.

For details about the configuration, see the configuration files.

Step 4 Verify the configuration.

After the configurations are complete and network become stable, run the following commands to verify the configuration. LSW1 is taken as an example.

- Run the **shutdown** command on XGE0/0/1 of LSW2 to simulate a port fault, and then run the display sep interface command on LSW3 to check whether XGE0/0/2 of LSW3 switches from the Discarding state to the Forwarding state.

  ```
  <LSW3> display sep interface xgigabitethernet 0/0/2
  SEP segment 1
  ------------------------------------------------------------------
  Interface           Port Role     Neighbor Status     Port Status
  ------------------------------------------------------------------
  XGE0/0/2             common        up                  forwarding
  ```

----End

Configuration Files

- Configuration file of LSW1

  ```
  #
   sysname LSW1
  #
   vlan batch 10 100
  ```

```
#
sep segment 1
 control-vlan 10
 block port middle
 tc-notify stp
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1 no-neighbor edge primary
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

- Configuration file of LSW2

```
#
 sysname LSW2
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 tc-notify stp
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1 no-neighbor edge secondary
#
return
```

- Configuration file of LSW3

```
#
 sysname LSW3
#
 vlan batch 10 100
#
sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan vlan 100
#
return
```

- Configuration file of PE1

```
#
 sysname PE1
```

```
#
 vlan batch 100
#
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 100
#
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 100
#
return
```

- Configuration file of PE3

```
#
 sysname PE3
#
 vlan batch 100 200
#
 stp instance 0 root primary
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
return
```

- Configuration file of PE4

```
#
 sysname PE4
#
 vlan batch 100 200
#
 stp instance 0 root secondary
 stp enable
#
 stp region-configuration
  region-name RG1
  active region-configuration
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid tagged vlan 100
 port hybrid untagged vlan 200
#
return
```

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
return
```

1.10.4 Example for Configuring SEP Multi-Instance on a Closed Ring Network

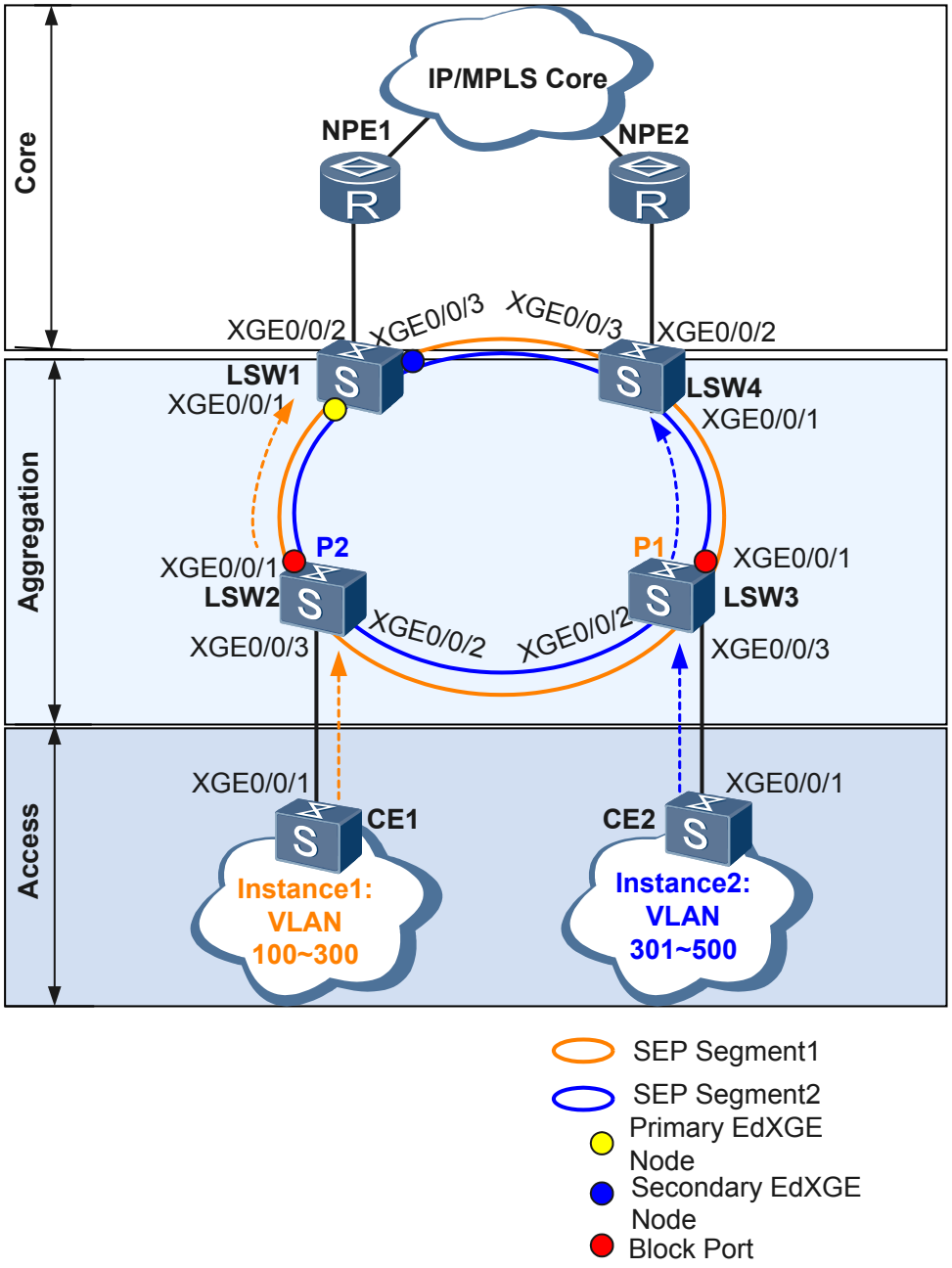
On a closed ring network, two SEP segments are configured to process different VLAN services, implement load balancing, and provide link backup.

Networking Requirements

In common SEP networking, a physical ring can be configured with only one SEP segment in which only one interface can be blocked. If an interface in the SEP segment in the complete state is blocked, all user data is transmitted only along the path where the primary edge interface is located. The path where the secondary edge interface is located is idle, which leads to a waste of bandwidth.

To solve the problem of bandwidth waste and to implement traffic load balancing, Huawei develops SEP multi-instance.

Figure 1-31 Networking diagram for configuring SEP multi-instance on a closed ring network



As shown in **Figure 1-31**, a ring network comprising Layer 2 switches LSW1 to LSW5 is connected to a core network. SEP runs at the aggregation layer. SEP multi-instance is configured on LSW1 to LSW4. This allows two SEP segments to solve the problem of bandwidth waste, implement load balancing, and provide link backup.

Configuration Roadmap

The configuration roadmap is as follows:

1. Create two SEP segments and one control VLAN on LSW1 to LSW4.

Different SEP segments can use the same control VLAN.

2. Configure SEP protected instances, and set mappings between SEP protected instances and user VLANs to ensure that topology changes affect only corresponding VLANs.
3. Add all the devices on the ring network to the SEP segments, and configure XGE 0/0/1 as the primary edge interface and XGE 0/0/3 as the secondary edge interface on LSW1.
4. Enable the function of specifying an interface to block on the device where the primary edge interface resides.
5. Configure the SEP preemption mode to ensure that the specified blocked interface takes effect when a fault is rectified.
6. Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW4.

Data Preparation

To complete the configuration, you need the following data:

- ID of each SEP segment
- ID of a control VLAN
- role of each interface added to each SEP segment
- mode of blocking an interface
- preemption mode
- ID of each SEP protection instance

Procedure

Step 1 Configure basic SEP functions.

- Configure a SEP segment with the ID of 1 and a control VLAN with the ID of 10.

  # Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] quit
```

  # Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] quit
```

  # Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] quit
```

  # Configure LSW4.

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] quit
```

- Configure a SEP segment with the ID of 2 and a control VLAN with the ID of 10.

  # Configure LSW1.

```
[LSW1] sep segment 2
```

```
[LSW1-sep-segment2] control-vlan 10
[LSW1-sep-segment2] quit
```

Configure LSW2.

```
[LSW2] sep segment2
[LSW2-sep-segment2] control-vlan 10
[LSW2-sep-segment2] quit
```

Configure LSW3.

```
[LSW3] sep segment 2
[LSW3-sep-segment2] control-vlan 10
[LSW3-sep-segment2] quit
```

Configure LSW4.

```
[LSW4] sep segment 2
[LSW4-sep-segment2] control-vlan 10
[LSW4-sep-segment2] quit
```

NOTE

- The control VLAN must be a new one.
- The command used to create a common VLAN is automatically displayed in a configuration file.
- Each SEP segment must be configured with a control VLAN. After being added to a SEP segment configured with a control VLAN, an interface is added to the control VLAN automatically.

Step 2 Configure SEP protected instances, and then configure mappings between SEP protected instances and user VLANs.

Configure LSW1.

```
[LSW1] vlan batch 100 to 500
[LSW1] sep segment 1
[LSW1-sep-segment1] protected-instance 1
[LSW1-sep-segment1] quit
[LSW1] sep segment 2
[LSW1-sep-segment2] protected-instance 2
[LSW1-sep-segment2] quit
[LSW1] stp region-configuration
[LSW1-mst-region] instance 1 vlan 100 to 300
[LSW1-mst-region] instance 2 vlan 301 to 500
[LSW1-mst-region] active region-configuration
[LSW1-mst-region] quit
```

The configurations of LSW2 to LSW4 are similar to those of LSW1, and are not provided here. For details, see configuration files in this configuration example.

Step 3 Add all the devices on the ring network to the SEP segments and configure interface roles.

NOTE

By default, STP is enabled on a Layer 2 interface. Before adding an interface to a SEP segment, disable STP on the interface.

On LSW1, configure XGE 0/0/1 as the primary edge interface and XGE 0/0/3 as the secondary edge interface.

```
[LSW1] interface xgigabitethernet 0/0/1
[LSW1-XGigabitEthernet0/0/1] stp disable
[LSW1-XGigabitEthernet0/0/1] sep segment 1 edge primary
[LSW1-XGigabitEthernet0/0/1] sep segment 2 edge primary
[LSW1-XGigabitEthernet0/0/1] quit
[LSW1] interface xgigabitethernet 0/0/3
[LSW1-XGigabitEthernet0/0/3] stp disable
[LSW1-XGigabitEthernet0/0/3] sep segment 1 edge secondary
[LSW1-XGigabitEthernet0/0/3] sep segment 2 edge secondary
[LSW1-XGigabitEthernet0/0/3] quit
```

Configure LSW2.

```
[LSW2] interface xgigabitethernet 0/0/1
[LSW2-XGigabitEthernet0/0/1] stp disable
```

```
[LSW2-XGigabitEthernet0/0/1] sep segment 1
[LSW2-XGigabitEthernet0/0/1] sep segment 2
[LSW2-XGigabitEthernet0/0/1] quit
[LSW2] interface xgigabitethernet 0/0/2
[LSW2-XGigabitEthernet0/0/2] stp disable
[LSW2-XGigabitEthernet0/0/2] sep segment 1
[LSW2-XGigabitEthernet0/0/2] sep segment 2
[LSW2-XGigabitEthernet0/0/2] quit
```

Configure LSW3.

```
[LSW3] interface xgigabitethernet 0/0/1
[LSW3-XGigabitEthernet0/0/1] stp disable
[LSW3-XGigabitEthernet0/0/1] sep segment 1
[LSW3-XGigabitEthernet0/0/1] sep segment 2
[LSW3-XGigabitEthernet0/0/1] quit
[LSW3] interface xgigabitethernet 0/0/2
[LSW3-XGigabitEthernet0/0/2] stp disable
[LSW3-XGigabitEthernet0/0/2] sep segment 1
[LSW3-XGigabitEthernet0/0/2] sep segment 2
[LSW3-XGigabitEthernet0/0/2] quit
```

Configure LSW4.

```
[LSW4] interface xgigabitethernet 0/0/1
[LSW4-XGigabitEthernet0/0/1] stp disable
[LSW4-XGigabitEthernet0/0/1] sep segment 1
[LSW4-XGigabitEthernet0/0/1] sep segment 2
[LSW4-XGigabitEthernet0/0/1] quit
[LSW4] interface xgigabitethernet 0/0/3
[LSW4-XGigabitEthernet0/0/3] stp disable
[LSW4-XGigabitEthernet0/0/3] sep segment 1
[LSW4-XGigabitEthernet0/0/3] sep segment 2
[LSW4-XGigabitEthernet0/0/3] quit
```

After completing the preceding configurations, run the **display sep topology** command on LSW1 to view the topology of each SEP segment. You can see that the blocked interface is one of the last two interfaces that complete neighbor negotiation.

```
[LSW1] display sep topology
SEP segment 1
------------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
------------------------------------------------------------------
LSW1                 XGE0/0/1          primary         forwarding
LSW2                 XGE0/0/1          common          forwarding
LSW2                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/3          common          forwarding
LSW1                 XGE0/0/3          secondary       discarding

SEP segment 2
------------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
------------------------------------------------------------------
LSW1                 XGE0/0/1          primary         forwarding
LSW2                 XGE0/0/1          common          forwarding
LSW2                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/3          common          forwarding
LSW1                 XGE0/0/3          secondary       discarding
```

Step 4 Specify an interface to block.

Configure delayed preemption and the mode of blocking an interface to be based on the device name and interface name on LSW1 where the primary edge interface is located.

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port sysname LSW3 interface xgigabitethernet 0/0/1
[LSW1-sep-segment1] preempt delay 15
[LSW1-sep-segment1] quit
[LSW1] sep segment 2
[LSW1-sep-segment2] block port sysname LSW2 interface xgigabitethernet 0/0/1
[LSW1-sep-segment2] preempt delay 15
[LSW1-sep-segment2] quit
```

NOTE

- In this configuration example, an interface fault needs to be simulated and then rectified to implement delayed preemption. To ensure that delayed preemption takes effect on the two SEP segments, simulate an interface fault in the two SEP segment. For example:
  - In SEP segment 1, run the **shutdown** command on XGE 0/0/1 of LSW2 to simulate an interface fault. Then, run the **undo shutdown** command on XGE 0/0/1 to simulate interface fault recovery.
  - In SEP segment 2, run the **shutdown** command on XGE 0/0/1 of LSW3 to simulate an interface fault. Then, run the **undo shutdown** command on XGE 0/0/1 to simulate interface fault recovery.

After completing the preceding operations, view SEP topologies. Use the display on LSW1 as an example.

Run the **display sep topology** command on LSW1. You can view information about the topology of each SEP segment.

```
[LSW1] display sep topology
SEP segment 1
------------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
------------------------------------------------------------------
LSW1                 XGE0/0/1          primary         forwarding
LSW2                 XGE0/0/1          common          forwarding
LSW2                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/1          common          discarding
LSW4                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/3          common          forwarding
LSW1                 XGE0/0/3          secondary       forwarding

SEP segment 2
------------------------------------------------------------------
System Name          Port Name        Port Role       Port Status
------------------------------------------------------------------
LSW1                 XGE0/0/1          primary         forwarding
LSW2                 XGE0/0/1          common          discarding
LSW2                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/2          common          forwarding
LSW3                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/1          common          forwarding
LSW4                 XGE0/0/3          common          forwarding
LSW1                 XGE0/0/3          secondary       forwarding
```

From the preceding command output, you can see:

- On LSW3 in SEP segment 1, XGE 0/0/1 is in the **discarding** state, and the other interfaces are in the **forwarding** state.
- On LSW2 in SEP segment 2, XGE 0/0/1 is in the **discarding** state, and the other interfaces are in the **forwarding** state.

Step 5 Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW4.

The configuration details are not provided here. For details, see configuration files in this example.

Step 6 Verify the configuration.

Simulate a fault, and then check whether the status of the blocked interface changes from blocked to forwarding.

Run the **shutdown** command on XGE 0/0/1 of LSW2 to simulate an interface fault.

Run the **display sep interface** command on LSW3 to check whether the status of XGE0/0/1 in SEP segment 1 changes from blocked to forwarding.

```
[LSW3] display sep interface xgigabitethernet 0/0/1
SEP segment 1
------------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
------------------------------------------------------------------
XGE0/0/1             common        up                  forwarding
SEP segment 2
------------------------------------------------------------------
Interface           Port Role     Neighbor Status     Port Status
------------------------------------------------------------------
XGE0/0/1             common        up                  forwarding
```

The preceding command output shows that the status of XGE 0/0/1 changes from blocked to forwarding and the forwarding path change in SEP segment 1 does not affect the forwarding path in SEP segment 2.

----End

Configuration Files

- Configuration file of LSW1

```
#
 sysname LSW1
#
 vlan batch 10 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
  active region-configuration
#
sep segment 1
 control-vlan 10
 block port sysname LSW3 interface XGigabitEthernet0/0/1
 preempt delay 15
 protected-instance 1
sep segment 2
 control-vlan 10
 block port sysname LSW2 interface XGigabitEthernet0/0/1
 preempt delay 15
 protected-instance 2
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1 edge primary
 sep segment 2 edge primary
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1 edge secondary
 sep segment 2 edge secondary
#
return
```

- Configuration file of LSW2

```
#
 sysname LSW2
#
 vlan batch 10 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
  active region-configuration
#
sep segment 1
 control-vlan 10
 protected-instance 1
sep segment 2
 control-vlan 10
 protected-instance 2
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 300
#
return
```

- Configuration file of LSW3

```
#
 sysname LSW3
#
 vlan batch 10 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
  active region-configuration
#
sep segment 1
 control-vlan 10
 protected-instance 1
sep segment 2
 control-vlan 10
 protected-instance 2
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
```

```
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 301 to 500
#
return
```

- Configuration file of LSW4

```
#
 sysname LSW4
#
 vlan batch 10 60 100 to 500
#
 stp region-configuration
  instance 1 vlan 100 to 300
  instance 2 vlan 301 to 500
  active region-configuration
#
sep segment 1
 control-vlan 10
 protected-instance 1
sep segment 2
 control-vlan 10
 protected-instance 2
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 100 to 500
 stp disable
 sep segment 1
 sep segment 2
#
return
```

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100 to 300
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 300
#
return
```

- Configuration file of CE2

```
#
 sysname CE2
#
 vlan batch 301 to 500
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 301 to 500
#
return
```

1.11 Layer 2 Protocol Transparent Transmission Configuration

This chapter describes the concept, configuration procedure, and configuration examples of Layer 2 protocol transparent transmission.

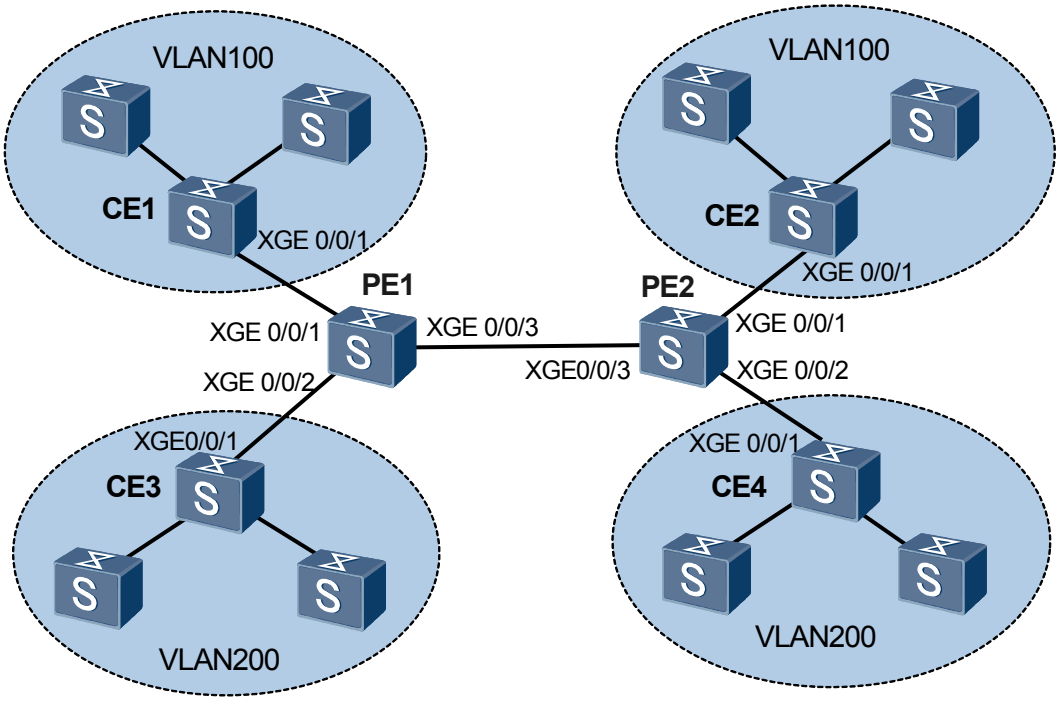
1.11.1 Example for Configuring Interface-based Layer 2 Protocol Transparent Transmission

Networking Requirements

As shown in **Figure 1-32**, CEs on user networks communicate with each other through PEs and STP runs on user networks; therefore, STP packets sent from CEs must be transmitted through the backbone network between PEs. Each PE interface is connected to only one CE and receives STP packets from the CE. In this scenario, configure interface-based Layer 2 protocol transparent transmission.

In this example, PEs on the backbone network transparently transmit STP packets sent from CEs by replacing the original multicast destination MAC address of STP packets with a specified MAC address. By default, the destination MAC address of STP packets is 0180-C200-0000.

Figure 1-32 Networking of interface-based Layer 2 protocol transparent transmission



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure STP on CEs.
2. Add user-side interfaces of PEs to the specified VLANs.
3. Configure interface-based Layer 2 protocol transparent transmission on PEs.
4. Configure network-side interfaces of PEs to allow packets of VLAN 100 and VLAN 200 to pass.

Data Preparation

To complete the configuration, you need the following data:

- IDs of VLANs that user-side interfaces of PEs belong to
- IDs of VLANs allowed by network-side interfaces of PEs

Procedure

Step 1 Enable STP on CEs and PEs.

Configure CE1.

```
<Quidway> system-view
[Quidway] sysname CE1
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] stp enable
[CE1] interface xgigabitethernet 0/0/1
[CE1-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[CE1-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[CE1-XGigabitEthernet0/0/1] bpdu enable
```

Configure CE2.

```
<Quidway> system-view
[Quidway] sysname CE2
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] stp enable
[CE2] interface xgigabitethernet 0/0/1
[CE2-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[CE2-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[CE2-XGigabitEthernet0/0/1] bpdu enable
```

Configure CE3.

```
<Quidway> system-view
[Quidway] sysname CE3
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] stp enable
[CE3] interface xgigabitethernet 0/0/1
[CE3-XGigabitEthernet0/0/1] port hybrid pvid vlan 200
[CE3-XGigabitEthernet0/0/1] port hybrid untagged vlan 200
[CE3-XGigabitEthernet0/0/1] bpdu enable
```

Configure CE4.

```
<Quidway> system-view
[Quidway] sysname CE4
[CE4] vlan 200
[CE4-vlan200] quit
```

```
[CE4] stp enable
[CE4] interface xgigabitethernet 0/0/1
[CE4-XGigabitEthernet0/0/1] port hybrid pvid vlan 200
[CE4-XGigabitEthernet0/0/1] port hybrid untagged vlan 200
[CE4-XGigabitEthernet0/0/1] bpdu enable
```

Configure PE1.

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1]
```

Configure PE2.

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2]
```

Step 2 On PE1 and PE2, add XGE 0/0/1 to VLAN 100, add XGE 0/0/2 to VLAN 200, and enable Layer 2 protocol transparent transmission.

Configure PE1.

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] interface XGigabitEthernet 0/0/1
[PE1-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[PE1-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[PE1-XGigabitEthernet0/0/1] l2protocol-tunnel stp enable
[PE1-XGigabitEthernet0/0/1] bpdu enable
[PE1-XGigabitEthernet0/0/1] quit
[PE1] vlan 200
[PE1-vlan200] quit
[PE1] interface XGigabitEthernet 0/0/2
[PE1-XGigabitEthernet0/0/2] port hybrid pvid vlan 200
[PE1-XGigabitEthernet0/0/2] port hybrid untagged vlan 200
[PE1-XGigabitEthernet0/0/2] l2protocol-tunnel stp enable
[PE1-XGigabitEthernet0/0/2] bpdu enable
[PE1-XGigabitEthernet0/0/2] quit
```

Configure PE2.

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] interface XGigabitEthernet 0/0/1
[PE2-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[PE2-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[PE2-XGigabitEthernet0/0/1] l2protocol-tunnel stp enable
[PE2-XGigabitEthernet0/0/1] bpdu enable
[PE2-XGigabitEthernet0/0/1] quit
[PE2] vlan 200
[PE2-vlan200] quit
[PE2] interface XGigabitEthernet 0/0/2
[PE2-XGigabitEthernet0/0/2] port hybrid pvid vlan 200
[PE2-XGigabitEthernet0/0/2] port hybrid untagged vlan 200
[PE2-XGigabitEthernet0/0/2] l2protocol-tunnel stp enable
[PE2-XGigabitEthernet0/0/2] bpdu enable
[PE2-XGigabitEthernet0/0/2] quit
```

Step 3 Configure PEs to replace the destination MAC address of STP packets received from CEs.

Configure PE1.

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

Configure PE2.

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

Step 4 On PE1 and PE2, configure network-side interface XGE 0/0/3 to allow packets of VLAN 100 and VLAN 200 to pass.

Configure PE1.

```
[PE1] interface xgigabitethernet 0/0/3
[PE1-XGigabitEthernet0/0/3] port hybrid tagged vlan 100 200
[PE1-XGigabitEthernet0/0/3] quit
```

Configure PE2.

```
[PE2] interface xgigabitethernet 0/0/3
[PE2-XGigabitEthernet0/0/3] port hybrid tagged vlan 100 200
[PE2-XGigabitEthernet0/0/3] quit
```

Step 5 Verify the configuration.

After the configuration, run the **display l2protocol-tunnel group-mac** command, and you can view the protocol type or name, original destination MAC address, new destination MAC address, and priority of Layer 2 protocol packets to be transparently transmitted.

Take the display on PE1 as an example.

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

Run the **display stp** command on CE1 and CE2 to view the root in the MST region. You can find that a spanning tree is calculated between CE1 and CE2. XGE 0/0/1 of CE1 is a root port, and CE 0/0/1 of CE2 is a designated port.

```
<CE1> display stp
-------[CIST Global Info] [Mode MSTP] -------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :6
TC count per hello  :6
STP Converge Mode   :Normal
Time since last TC received :0 days 2h:24m:36s
----[Port1(XGigabitEthernet0/0/1)] [FORWARDING] ----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :6
          TCN: 0, Config: 0, RST: 0, MST: 6
 BPDU Received       :4351
          TCN: 0, Config: 0, RST: 0, MST: 4351
<CE2> display stp
-------[CIST Global Info] [Mode MSTP] -------
CIST Bridge         :32768.00e0-fc9a-4315
```

```
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :3
TC count per hello  :3
STP Converge Mode   :Normal
Time since last TC received :0 days 2h:26m:42s
----[Port1(XGigabitEthernet0/0/1)] [FORWARDING] ----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :4534
          TCN: 0, Config: 0, RST: 0, MST: 4534
 BPDU Received       :6
          TCN: 0, Config: 0, RST: 0, MST: 6
```

Run the **display stp** command on CE3 and CE4 to view the root in the MST region. You can find that a spanning tree is calculated between CE3 and CE4. XGE 0/0/1 of CE3 is a root port, and CE 0/0/1 of CE4 is a designated port.

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-0967-58a0
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-0952-f13e / 199999
CIST RegRoot/IRPC   :32768.000b-0967-58a0 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC received :0 days 10h:54m:37s
----[Port1(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-0952-f13e / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :114
          TCN: 0, Config: 0, RST: 0, MST: 114
 BPDU Received       :885
          TCN: 0, Config: 0, RST: 0, MST: 885
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-0952-f13e
```

```
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-0952-f13e / 0
CIST RegRoot/IRPC   :32768.000b-0952-f13e / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
Time since last TC received :0 days 8h:59m:18s
----[Port1(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-0952-f13e / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :1834
          TCN: 0, Config: 0, RST: 0, MST: 1834
 BPDU Received       :1
          TCN: 0, Config: 0, RST: 0, MST: 1
```

----End

Configuration Files

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- Configuration file of CE2

```
#
 sysname CE2
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- Configuration file of CE3

```
#
 sysname CE3
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
```

```
return
```

- Configuration file of CE4

```
#
 sysname CE4
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
return
```

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 l2protocol-tunnel stp enable
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
 l2protocol-tunnel stp enable
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 100 200
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 l2protocol-tunnel stp enable
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
 l2protocol-tunnel stp enable
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 100 200
#
return
```

1.11.2 Example for Configuring VLAN-based Layer 2 Protocol Transparent Transmission

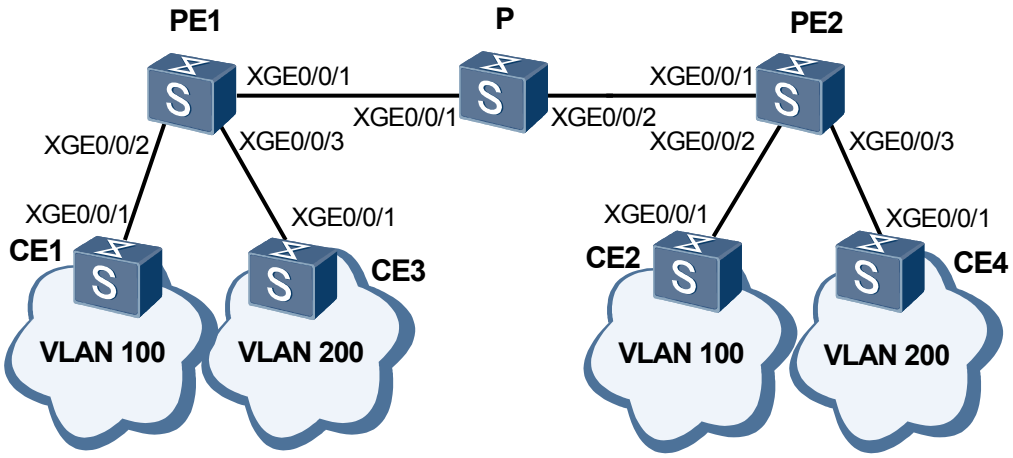
Networking Requirements

As shown in **Figure 1-33**, CEs on user networks communicate with each other through PEs and STP runs on user networks; therefore, STP packets sent from CEs must be transmitted through the backbone network between PEs. Each PE interface is an aggregation interface. PEs identify STP packets from different user networks according to VLAN tags of STP packets. In this scenario, configure VLAN-based Layer 2 protocol transparent transmission to ensure that:

- All the devices in VLAN 100 participate in calculation of a spanning tree.
- All the devices in VLAN 200 participate in calculation of a spanning tree.

In this example, PEs transparently transmit STP packets sent from user networks by replacing the original multicast destination MAC address of STP packets with a specified multicast MAC address. By default, the destination MAC address of STP packets is 0180-C200-0000.

Figure 1-33 Networking of VLAN-based Layer 2 protocol transparent transmission



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable STP on the CEs.
2. Configure CEs to send STP packets with specified VLAN tags to PEs.
3. Configure VLAN-based Layer 2 protocol transparent transmission on PEs.
4. Configure network-side interfaces of PEs to allow packets of VLAN 100 and VLAN 200 to pass.
5. Configure the Layer 2 forwarding function on the P device so that packets sent from PEs can be transmitted on the backbone network.

Data Preparation

To complete the configuration, you need the following data:

- VLAN tags in STP packets sent from CEs to PEs
- IDs of the VLANs that interfaces of PEs and CEs belong to

Procedure

Step 1 Enable STP on CEs and PEs.

Configure CE1.

```
[CE1] stp enable
```

Configure CE2.

```
[CE2] stp enable
```

Configure CE3.

```
[CE3] stp enable
```

Configure CE4.

```
[CE4] stp enable
```

Step 2 Configure CE1 and CE2 to send STP packets with VLAN tag 100 to PEs and configure CE3 and CE4 to send STP packets with VLAN tag 200 to PEs.

Configure CE1.

```
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface xgigabitethernet 0/0/1
[CE1-XGigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE1-XGigabitEthernet0/0/1] stp bpdu vlan 100
[CE1-XGigabitEthernet0/0/1] bpdu enable
```

Configure CE2.

```
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] interface xgigabitethernet 0/0/1
[CE2-XGigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE2-XGigabitEthernet0/0/1] stp bpdu vlan 100
[CE2-XGigabitEthernet0/0/1] bpdu enable
```

Configure CE3.

```
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] interface xgigabitethernet 0/0/1
[CE3-XGigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE3-XGigabitEthernet0/0/1] stp bpdu vlan 200
[CE3-XGigabitEthernet0/0/1] bpdu enable
```

Configure CE4.

```
[CE4] vlan 200
[CE4-vlan200] quit
[CE4] interface xgigabitethernet 0/0/1
[CE4-XGigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE4-XGigabitEthernet0/0/1] stp bpdu vlan 200
[CE4-XGigabitEthernet0/0/1] bpdu enable
```

Step 3 Configure PE interfaces to transparently transmit STP packets of CEs to the P device.

Configure PE1.

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] vlan 200
[PE1-vlan200] quit
[PE1] interface xgigabitethernet 0/0/1
[PE1-XGigabitEthernet0/0/1] port hybrid tagged vlan 100 200
```

```
[PE1-XGigabitEthernet0/0/1] quit
[PE1] interface xgigabitethernet 0/0/2
[PE1-XGigabitEthernet0/0/2] port hybrid tagged vlan 100
[PE1-XGigabitEthernet0/0/2] l2protocol-tunnel stp vlan 100
[PE1-XGigabitEthernet0/0/2] bpdu enable
[PE1-XGigabitEthernet0/0/2] quit
[PE1] interface xgigabitethernet 0/0/3
[PE1-XGigabitEthernet0/0/3] port hybrid tagged vlan 200
[PE1-XGigabitEthernet0/0/3] l2protocol-tunnel stp vlan 200
[PE1-XGigabitEthernet0/0/3] bpdu enable
[PE1-XGigabitEthernet0/0/3] quit
```

Configure PE2.

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] vlan 200
[PE2-vlan200] quit
[PE2] interface xgigabitethernet 0/0/1
[PE2-XGigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[PE2-XGigabitEthernet0/0/1] quit
[PE2] interface xgigabitethernet 0/0/2
[PE2-XGigabitEthernet0/0/2] port hybrid tagged vlan 100
[PE2-XGigabitEthernet0/0/2] l2protocol-tunnel stp vlan 100
[PE2-XGigabitEthernet0/0/2] bpdu enable
[PE2-XGigabitEthernet0/0/2] quit
[PE2] interface xgigabitethernet 0/0/3
[PE2-XGigabitEthernet0/0/3] port hybrid tagged vlan 200
[PE2-XGigabitEthernet0/0/3] l2protocol-tunnel stp vlan 200
[PE2-XGigabitEthernet0/0/3] bpdu enable
[PE2-XGigabitEthernet0/0/3] quit
```

Step 4 Configure PEs to replace the destination MAC address of STP packets received from CEs.

Configure PE1.

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

Configure PE2.

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

Step 5 Configure the Layer 2 forwarding function on the P device and configure it to allow packets of VLAN 100 and VLAN 200 to pass.

```
[P] vlan 100
[P-vlan100] quit
[P] vlan 200
[P-vlan200] quit
[P] interface xgigabitethernet 0/0/1
[P-XGigabitEthernet0/0/1] port hybrid tagged vlan 100 200
[P-XGigabitEthernet0/0/1] quit
[P] interface xgigabitethernet 0/0/2
[P-XGigabitEthernet0/0/2] port hybrid tagged vlan 100 200
[P-XGigabitEthernet0/0/2] quit
```

Step 6 Verify the configuration.

After the configuration, run the **display l2protocol-tunnel group-mac** command. You can view the protocol type or name, original destination MAC address, new destination MAC address, and priority of Layer 2 protocol packets to be transparently transmitted.

Take the ouput on PE1 as an example.

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

Run the **display stp** command on CE1 and CE2 to view the root in the MST region. You can find that a spanning tree is calculated between CE1 and CE2. XGE 0/0/1 of CE1 is a root port, and CE 0/0/1 of CE2 is a designated port.

```
<CE1> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09f0-1b91
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 199999
CIST RegRoot/IRPC   :32768.000b-09f0-1b91 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:53m:43s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :237
          TCN: 0, Config: 0, RST: 0, MST: 237
 BPDU Received       :9607
          TCN: 0, Config: 0, RST: 0, MST: 9607
<CE2> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09d4-b66c
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 0
CIST RegRoot/IRPC   :32768.000b-09d4-b66c / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :1
TC count per hello  :1
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:29m:6s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7095
          TCN: 0, Config: 0, RST: 0, MST: 7095
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

Run the **display stp** command on CE3 and CE4 to view the root in the MST region. You can find that a spanning tree is calculated between CE3 and CE4. XGE 0/0/1 of CE3 is a root port, and CE 0/0/1 of CE4 is a designated port.

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:57m:0s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :238
          TCN: 0, Config: 0, RST: 0, MST: 238
 BPDU Received       :9745
          TCN: 0, Config: 0, RST: 0, MST: 9745
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9a-4315
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:33m:17s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7171
          TCN: 0, Config: 0, RST: 0, MST: 7171
 BPDU Received       :2
```

```
TCN: 0, Config: 0, RST: 0, MST: 2
```

----End

Configuration Files

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- Configuration file of CE2

```
#
 sysname CE2
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- Configuration file of CE3

```
#
 sysname CE3
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- Configuration file of CE4

```
#
 sysname CE4
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
Return
```

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100
 l2protocol-tunnel stp vlan 100
```

```
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 200
 l2protocol-tunnel stp vlan 200
#
return
```

- Configuration file of P

```
#
 sysname P
#
 vlan batch 100 200
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100 200
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 100 200
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100 200
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100
 l2protocol-tunnel stp vlan 100
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 200
 l2protocol-tunnel stp vlan 200
#
return
```

1.11.3 Example for Configuring QinQ-based Layer 2 Protocol Transparent Transmission

Networking Requirements

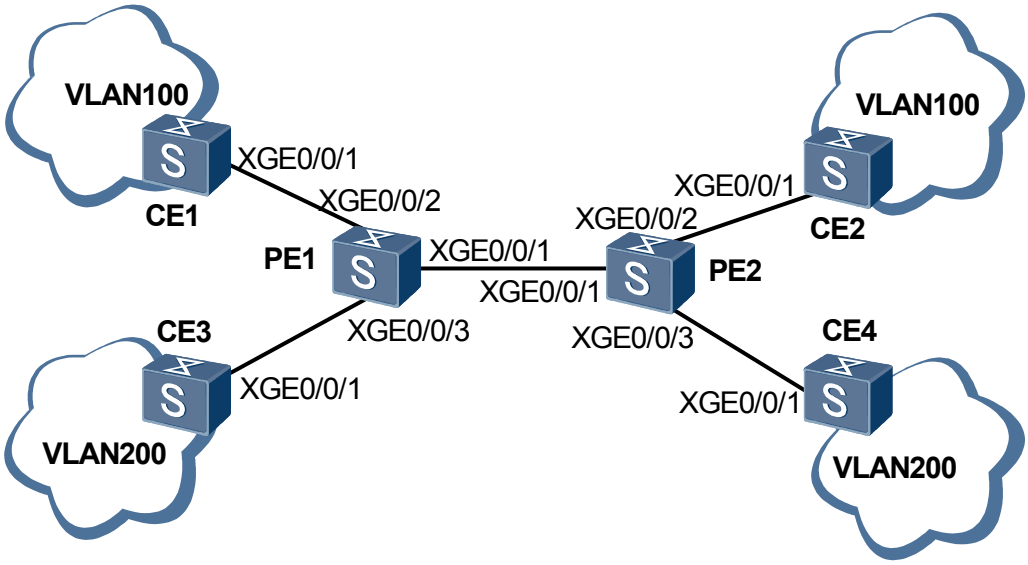
As shown in **Figure 1-34**, CEs on user networks communicate with each other through PEs. STP runs on user networks. CE1 and CE2 send STP packets with VLAN tag 100 to PEs; CE3 and CE4 send STP packets with VLAN tag 200 to PEs. In this scenario, configure QinQ-based Layer 2 protocol transparent transmission to ensure that:

- All the devices in VLAN 100 participate in calculation of a spanning tree.
- All the devices in VLAN 200 participate in calculation of a spanning tree.

To save VLAN IDs on the public network, configure VLAN stacking on PEs to add outer VLAN tag 10 to STP packets with VLAN tag 100 and VLAN tag 200. Then STP packets contain double tags and are transparently transmitted on the backbone network.

In this example, PEs transparently transmit STP packets sent from user networks by replacing the original multicast destination MAC address of STP packets with a specified multicast MAC address. By default, the destination MAC address of STP packets is 0180-C200-0000.

Figure 1-34 Networking of QinQ-based Layer 2 protocol transparent transmission



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable STP on the CEs.
2. Configure CEs to send STP packets with specified VLAN tags to PEs.
3. Configure VLAN-based Layer 2 protocol transparent transmission on PEs.
4. Configure QinQ (VLAN stacking) on PEs so that PEs add outer VLAN tag 10 to STP packets sent from CEs.

Data Preparation

To complete the configuration, you need the following data:

- VLAN tags in STP packets sent from CEs to PEs
- Outer VLAN tag that PEs add to STP packets
- IDs of the VLANs that interfaces of PEs and CEs belong to

Procedure

Step 1 Enable STP on CEs and PEs.

Configure CE1.

```
[CE1] stp enable
```

Configure CE2.

```
[CE2] stp enable
```

Configure CE3.

```
[CE3] stp enable
```

Configure CE4.

```
[CE4] stp enable
```

Step 2 Configure CE1 and CE2 to send STP packets with VLAN tag 100 to PEs and configure CE3 and CE4 to send STP packets with VLAN tag 200 to PEs.

Configure CE1.

```
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface xgigabitethernet 0/0/1
[CE1-XGigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE1-XGigabitEthernet0/0/1] stp bpdu vlan 100
[CE1-XGigabitEthernet0/0/1] bpdu enable
[CE1-XGigabitEthernet0/0/1] quit
```

Configure CE2.

```
[CE2] vlan 100
[CE2-vlan100] quit
[CE2] interface xgigabitethernet 0/0/1
[CE2-XGigabitEthernet0/0/1] port hybrid tagged vlan 100
[CE2-XGigabitEthernet0/0/1] stp bpdu vlan 100
[CE2-XGigabitEthernet0/0/1] bpdu enable
[CE2-XGigabitEthernet0/0/1] quit
```

Configure CE3.

```
[CE3] vlan 200
[CE3-vlan200] quit
[CE3] interface xgigabitethernet 0/0/1
[CE3-XGigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE3-XGigabitEthernet0/0/1] stp bpdu vlan 200
[CE3-XGigabitEthernet0/0/1] bpdu enable
[CE3-XGigabitEthernet0/0/1] quit
```

Configure CE4.

```
[CE4] vlan 200
[CE4-vlan200] quit
[CE4] interface xgigabitethernet 0/0/1
[CE4-XGigabitEthernet0/0/1] port hybrid tagged vlan 200
[CE4-XGigabitEthernet0/0/1] stp bpdu vlan 200
[CE4-XGigabitEthernet0/0/1] bpdu enable
[CE4-XGigabitEthernet0/0/1] quit
```

Step 3 Configure QinQ-based transparent transmission on PEs so that PEs add outer VLAN tag 10 to STP packets with VLAN tag 100 and VLAN tag 200.

Configure PE1.

```
[PE1] vlan 10
[PE1-Vlan10] quit
[PE1] interface xgigabitethernet 0/0/1
[PE1-XGigabitEthernet0/0/1] port hybrid tagged vlan 10
[PE1-XGigabitEthernet0/0/1] quit
[PE1] interface xgigabitethernet 0/0/2
[PE1-XGigabitEthernet0/0/2] qinq vlan-translation enable
[PE1-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[PE1-XGigabitEthernet0/0/2] port vlan-stacking vlan 100 stack-vlan 10
[PE1-XGigabitEthernet0/0/2] l2protocol-tunnel stp vlan 10
[PE1-XGigabitEthernet0/0/2] bpdu enable
[PE1-XGigabitEthernet0/0/2] quit
[PE1] interface xgigabitethernet 0/0/3
[PE1-XGigabitEthernet0/0/3] qinq vlan-translation enable
[PE1-XGigabitEthernet0/0/3] port hybrid untagged vlan 10
[PE1-XGigabitEthernet0/0/3] port vlan-stacking vlan 200 stack-vlan 10
[PE1-XGigabitEthernet0/0/3] l2protocol-tunnel stp vlan 10
```

```
[PE1-XGigabitEthernet0/0/3] bpdu enable
[PE1-XGigabitEthernet0/0/3] quit
```

Configure PE2.

```
[PE2] vlan 10
[PE2-Vlan10] quit
[PE2] interface xgigabitethernet 0/0/1
[PE2-XGigabitEthernet0/0/1] port hybrid tagged vlan 10
[PE2-XGigabitEthernet0/0/1] quit
[PE2] interface xgigabitethernet 0/0/2
[PE2-XGigabitEthernet0/0/2] qinq vlan-translation enable
[PE2-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[PE2-XGigabitEthernet0/0/2] port vlan-stacking vlan 100 stack-vlan 10
[PE2-XGigabitEthernet0/0/2] l2protocol-tunnel stp vlan 10
[PE2-XGigabitEthernet0/0/2] bpdu enable
[PE2-XGigabitEthernet0/0/2] quit
[PE2] interface xgigabitethernet 0/0/3
[PE2-XGigabitEthernet0/0/3] qinq vlan-translation enable
[PE2-XGigabitEthernet0/0/3] port hybrid untagged vlan 10
[PE2-XGigabitEthernet0/0/3] port vlan-stacking vlan 200 stack-vlan 10
[PE2-XGigabitEthernet0/0/3] l2protocol-tunnel stp vlan 10
[PE2-XGigabitEthernet0/0/3] bpdu enable
[PE2-XGigabitEthernet0/0/3] quit
```

Step 4 Configure PEs to replace the destination MAC address of STP packets received from CEs.

Configure PE1.

```
[PE1] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

Configure PE2.

```
[PE2] l2protocol-tunnel stp group-mac 0100-5e00-0011
```

Step 5 Verify the configuration.

After the configuration, run the **display l2protocol-tunnel group-mac** command. You can view the protocol type or name, original destination MAC address, new destination MAC address, and priority of Layer 2 protocol packets to be transparently transmitted.

Take the output on PE1 as an example.

```
<PE1> display l2protocol-tunnel group-mac stp
Protocol         EncapeType ProtocolType Protocol-MAC   Group-MAC      Pri
------------------------------------------------------------------------------
stp              llc        dsap 0x42    0180-c200-0000 0100-5e00-0011 0
                            ssap 0x42
```

Run the **display stp** command on CE1 and CE2 to view the root in the MST region. You can find that a spanning tree is calculated between CE1 and CE2. XGE 0/0/1 of CE1 is a root port, and CE 0/0/1 of CE2 is a designated port.

```
<CE1> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09f0-1b91
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 199999
CIST RegRoot/IRPC   :32768.000b-09f0-1b91 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:53m:43s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
```

```
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :237
          TCN: 0, Config: 0, RST: 0, MST: 237
 BPDU Received       :9607
          TCN: 0, Config: 0, RST: 0, MST: 9607
<CE2> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.000b-09d4-b66c
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.000b-09d4-b66c / 0
CIST RegRoot/IRPC   :32768.000b-09d4-b66c / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :1
TC count per hello  :1
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:29m:6s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.000b-09d4-b66c / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7095
          TCN: 0, Config: 0, RST: 0, MST: 7095
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

Run the **display stp** command on CE3 and CE4 to view the root in the MST region. You can find that a spanning tree is calculated between CE3 and CE4. XGE 0/0/1 of CE3 is a root port, and CE 0/0/1 of CE4 is a designated port.

```
<CE3> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9f-3257
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 199999
CIST RegRoot/IRPC   :32768.00e0-fc9f-3257 / 0
CIST RootPortId     :128.82
BPDU-Protection     :disabled
TC or TCN received  :4
TC count per hello  :4
STP Converge Mode   :Normal
Time since last TC received :0 days 3h:57m:0s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Root Port
```

```
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :238
          TCN: 0, Config: 0, RST: 0, MST: 238
 BPDU Received       :9745
          TCN: 0, Config: 0, RST: 0, MST: 9745
<CE4> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc9a-4315
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc9a-4315 / 0
CIST RegRoot/IRPC   :32768.00e0-fc9a-4315 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
TC or TCN received  :2
TC count per hello  :2
STP Converge Mode   :Normal
Time since last TC received :0 days 5h:33m:17s
----[Port17(XGigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000000
 Desg. Bridge/Port   :32768.00e0-fc9a-4315 / 128.82
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port Stp Mode       :MSTP
 Port Protocol Type  :Config=auto / Active= dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :7171
          TCN: 0, Config: 0, RST: 0, MST: 7171
 BPDU Received       :2
          TCN: 0, Config: 0, RST: 0, MST: 2
```

Run the **display vlan** command on PEs to view the QinQ configuration.

Take the output on PE1 as an example.

```
<PE1> display vlan 10 verbose
* : Management-VLAN
----------------------
VLAN ID      : 10
VLAN Type    : Common
Description  : VLAN 0010
Status       : Enable
Broadcast    : Enable
MAC Learning : Enable
Statistics   : Disable
Property     : Default
VLAN State   : Up
----------------
Tagged        Port: XGigabitEthernet0/0/1
----------------
```

```
QinQ-stack    Port: XGigabitEthernet0/0/2
XGigabitEthernet0/0/3
```

----End

Configuration Files

- Configuration file of CE1

```
#
 sysname CE1
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- Configuration file of CE2

```
#
 sysname CE2
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
 stp bpdu vlan 100
#
return
```

- Configuration file of CE3

```
#
 sysname CE3
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- Configuration file of CE4

```
#
 sysname CE4
#
 vlan batch 200
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 200
 stp bpdu vlan 200
#
return
```

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface XGigabitEthernet0/0/2
 qinq vlan-translation enable
```

```
 port hybrid untagged vlan 10
 port vlan-stacking vlan 100 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
interface XGigabitEthernet0/0/3
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 200 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 10
#
 l2protocol-tunnel stp group-mac 0100-5e00-0011
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface XGigabitEthernet0/0/2
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 100 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
interface XGigabitEthernet0/0/3
 qinq vlan-translation enable
 port hybrid untagged vlan 10
 port vlan-stacking vlan 200 stack-vlan 10
 l2protocol-tunnel stp vlan 10
#
return
```

2 Configuration Guide - IP Service

About This Chapter

This document describes the configurations of the IP services of the S6700, including the basic knowledge and configurations of secondary IP addresses, DNS, IPv6 DNS, ARP, DHCP, IP performance, DHCP Policy VLAN, basic IPv6 functions, and IPv6 over IPv4 tunnels. By reading this document, you can learn the concepts and configuration procedures of IP services.

2.1 IP Addresses Configuration
By assigning IP addresses to network devices, you can enable data communications between the network devices.

2.2 ARP Configuration
ARP can map an IP address to a MAC address and implements transmission of Ethernet frames.

2.3 DHCP Configuration
The DHCP technology is applicable to a variety of networks. It ensures proper IP address allocation and saves IP addresses on networks.

2.4 DHCPv6 Configuration
Currently, the S6700 can function as only the DHCP relay agent on IPv6 networks. This document describes how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay.

2.5 IP Performance Configuration
This chapter describes the basic concepts of IP performance, and provides configuration procedures and examples of IP performance.

2.6 DHCP Policy VLAN Configuration
This chapter describes the concept, operating mode, and configuration of Dynamic Host Configuration Protocol (DHCP) policy Virtual Local Area Network (VLAN), and provides configuration examples.

2.7 DNS Configuration
By configuring the Domain Name System (DNS), you can enable network devices to communicate with other through their domain names.

2.8 Basic Configurations of IPv6
This chapter describes the basic concept and configurations of IPv6.

2.9 IPv6 DNS Configuration

By configuring the IPv6 Domain Name System (DNS), you can enable network devices to communicate with other through their domain names.

2.10 IPv6 over IPv4 Tunnel Configuration

The IPv6 over IPv4 tunnel technology is developed to address the problem in the transition from IPv4 networks to IPv6 networks.

2.1 IP Addresses Configuration

By assigning IP addresses to network devices, you can enable data communications between the network devices.

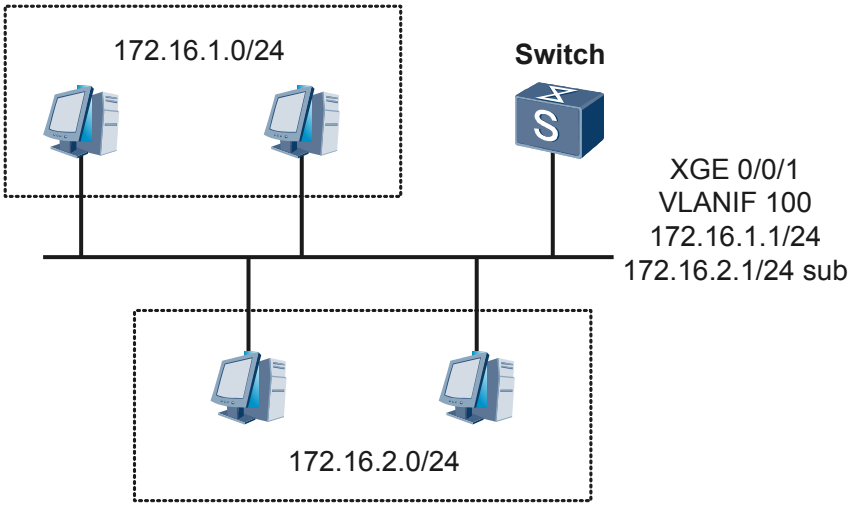
2.1.1 Example for Setting Primary and Secondary IP Addresses

This section provides a configuration example of setting primary and secondary IP addresses.

Networking Requirements

As shown in **Figure 2-1**, XGigabitEthernet 0/0/1 of the Switch is connected to a LAN, in which hosts belong to two different network segments, that is 172.16.1.0/24 and 172.16.2.0/24. It is required that the Switch can access the two network segments but the host in 172.16.1.0/24 cannot interconnect with the host in 172.16.2.0/24.

Figure 2-1 Networking diagram for setting IP addresses



Configuration Roadmap

The configuration roadmap is as follows:

1. Analyze the address of the network segment to which each interface is connected.
2. Set the secondary IP addresses for an interface.

Data Preparation

To complete the configuration, you need the following data.

- Primary IP address and subnet mask of the VLANIF interface
- Secondary IP address and subnet mask of the VLANIF interface

Procedure

Step 1 Set the IP address for VLANIF 100 where XGigabitEthernet 0/0/1 of the Switch belongs.

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-Vlan100] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ip address 172.16.1.1 24
[Quidway-Vlanif100] ip address 172.16.2.1 24 sub
```

Step 2 Verify the configuration.

Ping a host on network segment 172.16.2.0 from Switch. The ping succeeds.

```
<Quidway> ping 172.16.1.2
PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=128 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/26/27 ms
```

Ping a host on network segment 172.16.2.0 from the Switch. The ping succeeds.

```
<Quidway> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan 100
#
interface Vlanif100
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 sub
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

2.2 ARP Configuration

ARP can map an IP address to a MAC address and implements transmission of Ethernet frames.

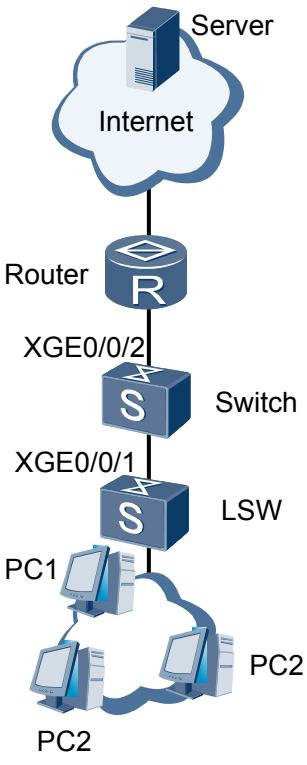
2.2.1 Example for Configuring ARP

Networking Requirements

As shown in **Figure 2-2**, XGE 0/0/1 of the Switch is connected to the host through the LAN switch (LSW); XGE 0/0/2 is connected to the server through the router. It is required that:

- XGE 0/0/1 should be added to VLAN 2, and XGE 0/0/2 should be added to VLAN 3.
- To adapt to fast changes of the network and ensure correct forwarding of packets, dynamic ARP parameters should be set on VLANIF 2 of the Switch.
- To ensure the security of the server and prevent invalid ARP packets, a static ARP entry should be created on XGE 0/0/2 of the Switch, with the IP address of the router being 10.2.2.3 and the MAC address being 00e0-fc01-0000.

Figure 2-2 Networking diagram for configuring ARP



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and add an interface to the VLAN.
2. Set dynamic ARP parameters on a VLANIF interface at the user side.
3. Create a static ARP entry.

Data Preparation

To complete the configuration, you need the following data:

- XGE 0/0/1 added to VLAN 2 and XGE 0/0/2 added to VLAN 3
- VLANIF 2 with the IP address being 2.2.2.2 and subnet mask being 255.255.255.0, aging time of ARP entries being 60s, and number of detection times being 2
- VLANIF 3 with the IP address being 10.2.2.2 and subnet mask being 255.255.255.0
- Interface connecting the router and the Switch, with the IP address being 10.2.2.3, subnet mask being 255.255.255.0, and MAC address being 00e0-fc01-0000

Procedure

Step 1 Create a VLAN and add an interface to the VLAN.

Create VLAN 2 and VLAN 3.

```
<Quidway> system-view
[Quidway] vlan batch 2 3
```

Add XGE 0/0/1 to VLAN 2 and add XGE 0/0/2 to VLAN 3.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid tagged vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid tagged vlan 3
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 Set dynamic ARP parameters on a VLANIF interface.

Create VLANIF2.

```
[Quidway] interface vlanif 2
```

Assign an IP address to VLANIF 2.

```
[Quidway-Vlanif2] ip address 2.2.2.2 255.255.255.0
```

Set the aging time of ARP entries to 60s.

```
[Quidway-Vlanif2] arp expire-time 60
```

Set the number of detection times before deleting ARP entries to 2.

```
[Quidway-Vlanif2] arp detect-times 2
[Quidway-Vlanif2] quit
```

Create VLANIF 3.

```
[Quidway] interface vlanif 3
```

Assign an IP address to VLANIF 3.

```
[Quidway-Vlanif3] ip address 10.2.2.2 255.255.255.0
[Quidway-Vlanif3] quit
```

Step 3 Create a static ARP entry.

Create a static ARP entry with IP address 10.2.2.3, MAC address 00e0-fc01-0000, VLAN ID 3, and outgoing interface XGE 0/0/2.

```
[Quidway] arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface xgigabitethernet
0/0/2
[Quidway] quit
```

Step 4 Verify the configuration.

Run the **display current-configuration** command. You can view the aging time of ARP entries, the number of detection times before deleting ARP entries, and the ARP mapping table.

```
<Quidway> display current-configuration | include arp
 arp expire-time 60
 arp detect-times 2
 arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface XGigabitEthernet0/0/2
```

----End

Configuration Files

The following is the configuration file of the Switch.

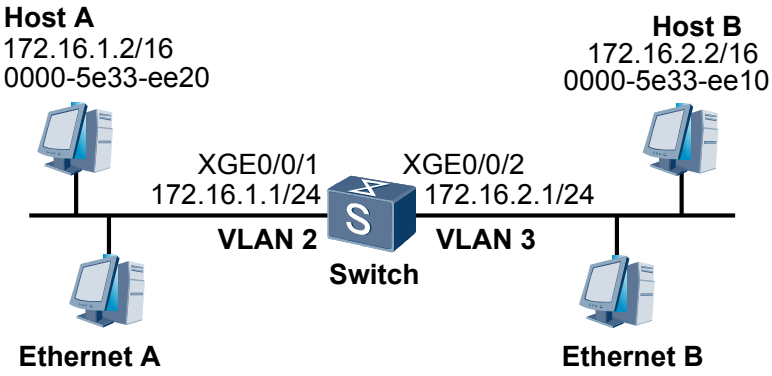
```
#
 sysname Quidway
#
vlan batch 2 to 3
#
interface Vlanif2
 ip address 2.2.2.2 255.255.255.0
 arp expire-time 60
 arp detect-times 2
#
interface Vlanif3
 ip address 10.2.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 2
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 3
#
 arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface XGigabitEthernet0/0/2
#
return
```

2.2.2 Example for Configuring Routed Proxy ARP

Networking Requirements

As shown in **Figure 2-3**, XGE 0/0/1 and XGE 0/0/2 of the Switch are connected to a LAN respectively, and the network IDs of the two LANs are 172.16.0.0/16. Host A and Host B are not configured with the default gateway. It is required that routed proxy ARP should be enabled on the Switch so that hosts in the two LANs can communicate.

Figure 2-3 Networking diagram for configuring routed proxy ARP



Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP Address to an interface.
2. Enable routed proxy ARP on the interface.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the interfaces
- IP addresses of the hosts

Procedure

Step 1 Create VLAN 2 and add XGE 0/0/1 to VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
[Quidway-XGigabitEthernet0/0/1] port default vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Create and configure VLANIF 2.

```
[Quidway]  interface vlanif 2
[Quidway-Vlanif2] ip address 172.16.1.1 255.255.255.0
```

Step 3 Enable routed proxy ARP on VLANIF 2.

```
[Quidway-Vlanif2] arp-proxy enable
[Quidway-Vlanif2] quit
```

Step 4 Create VLAN 3 and add XGE 0/0/2 to VLAN 3.

```
[Quidway] vlan 3
[Quidway-vlan3] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 3
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 5 Create and configure VLANIF 3.

```
[Quidway] interface vlanif 3
[Quidway-Vlanif3] ip address 172.16.2.1 255.255.255.0
```

Step 6 Enable routed proxy ARP on VLANIF 3.

```
[Quidway-Vlanif3] arp-proxy enable
[Quidway-Vlanif3] quit
```

Step 7 Configure the hosts.

Assign IP address 172.16.1.2/16 to Host A.

Assign IP address 172.16.2.2/16 to Host B.

Step 8 Verify the configuration.

Ping Host B from Host A. The ping operation is successful.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
interface Vlanif2
 ip address 172.16.1.1 255.255.255.0
 arp-proxy enable
#
interface Vlanif3
 ip address 172.16.2.1 255.255.255.0
 arp-proxy enable
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 3
#
return
```

2.2.3 Example for Configuring Intra-VLAN Proxy ARP

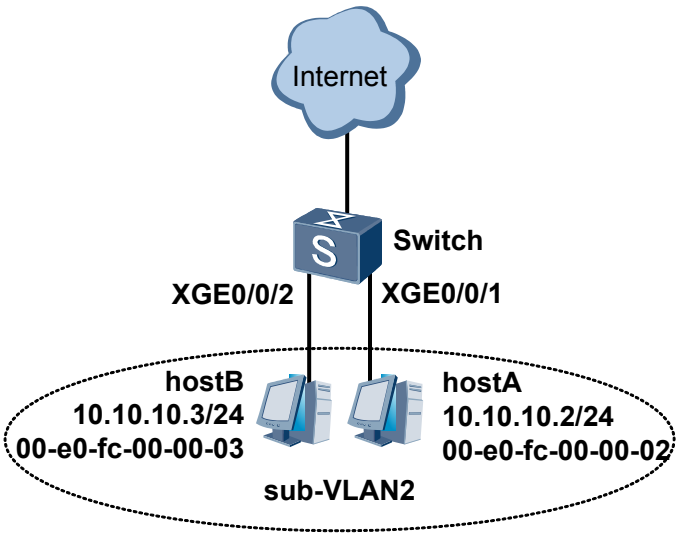
Networking Requirements

As shown in **Figure 2-4**, XGE 0/0/2 and XGE 0/0/1 of the Switch belong to Sub-VLAN 2. Sub-VLAN 2 belong to Super-VLAN 3. It is required that:

- Host A and host B in VLAN 2 should be isolated at Layer 2.
- Host A should communicate with host B at Layer 3 through intra-VLAN proxy ARP.

The IP address and subnet mask of the VLANIF interface in Super-VLAN 3 should be 10.10.10.1 and 255.255.255.0.

Figure 2-4 Networking diagram for configuring intra-VLAN proxy ARP



Configuration Roadmap

The configuration roadmap is as follows:

1. Create and configure a Super-VLAN and a Sub-VLAN.
2. Add an interface to the Sub-VLAN.
3. Create a VLANIF interface of the Super-VLAN and assign an IP address to the VLANIF interface.
4. Enable intra-VLAN proxy ARP on the VLANIF interface of the Super-VLAN.

Data Preparation

To complete the configuration, you need the following data:

- VLAN IDs of the Super-VLAN and Sub-VLAN
- XGE 0/0/2 and XGE 0/0/1 belonging to Sub-VLAN 2
- IP address and subnet mask of VLANIF 3 of Super-VLAN 3 being 10.10.10.1 and 255.255.255.0

Procedure

Step 1 Configure the Super-VLAN and Sub-VLAN.

Configure Sub-VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

Enable port isolation on XGE 0/0/1 and XGE 0/0/2.

```
[Quidway] port-isolate mode l2
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port-isolate enable
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
```

```
[Quidway-XGigabitEthernet0/0/2] port-isolate enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/1 and XGE 0/0/2 to Sub-VLAN 2.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
[Quidway-XGigabitEthernet0/0/1] port default vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 2
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure Super-VLAN 3 and add Sub-VLAN 2 to Super-VLAN 3.

```
[Quidway] vlan 3
[Quidway-vlan3] aggregate-vlan
[Quidway-vlan3] access-vlan 2
[Quidway-vlan3] quit
```

Step 2 Create and configure VLANIF 3.

Create VLANIF 3.

```
[Quidway] interface vlanif 3
```

Assign an IP address to VLANIF 3.

```
[Quidway-Vlanif3] ip address 10.10.10.1 24
```

Step 3 Enable intra-VLAN proxy ARP on VLANIF 3.

```
[Quidway-Vlanif3] arp-proxy inner-sub-vlan-proxy enable
[Quidway-Vlanif3] quit
```

Step 4 Verify the configuration.

Run the **display current-configuration** command. You can view the configurations of the Super-VLAN, Sub-VLAN, and VLANIF interface. For query results, see the following configuration file.

Run the **display arp** command to view all the ARP entries.

```
<Quidway> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.10.10.1      0018-2000-0083            I -         Vlanif3
10.10.10.2      00e0-fc00-0002  19        D-0         XGE0/0/1
                                          2
10.10.10.3      00e0-fc00-0003  19        D-0         XGE0/0/2
                                          2
------------------------------------------------------------------------------
Total:3         Dynamic:2       Static:0    Interface:1
```

----End

Configuration Files

The following lists the configuration file of the Switch.

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
vlan 3
 aggregate-vlan
```

```
 access-vlan 2
#
interface Vlanif3
 ip address 10.10.10.1 255.255.255.0
 arp-proxy inner-sub-vlan-proxy enable
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 2
 port-isolate enable group 1
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 2
 port-isolate enable group 1
#
return
```

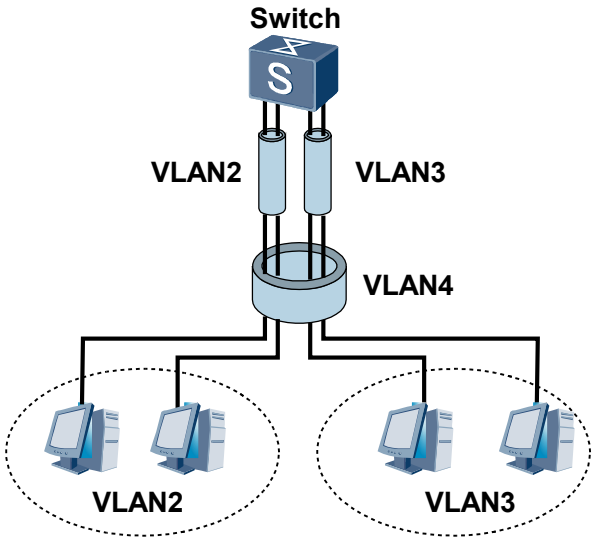
2.2.4 Example for Configuring Inter-VLAN Proxy ARP

Networking Requirements

As shown in **Figure 2-5**, VLAN 2 and VLAN 3 constitute super-VLAN 4. It is required that:

- Hosts in the sub-VLANs 2 and 3 should not be pinged mutually.
- Hosts in VLAN 2 and VLAN 3 should be pinged mutually after inter-VLAN proxy ARP is enabled.

Figure 2-5 Networking diagram for configuring inter-VLAN proxy ARP



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a super-VLAN and a sub-VLAN.
2. Add an interface to the sub-VLAN.

3. Create an VLANIF interface of the super-VLAN and assign an IP address to the VLANIF interface.
4. Enable inter-VLAN proxy ARP.

Data Preparation

To complete the configuration, you need the following data:

- VLAN IDs of the super-VLAN and sub-VLAN
- XGE 0/0/2 and XGE 0/0/1 belonging to sub-VLAN 2
- XGE 0/0/3 and XGE 0/0/4 belonging to sub-VLAN 3
- IP address and subnet mask of VLANIF 4 in super-VLAN 4 being 10.10.10.1 and 255.255.255.0

Procedure

Step 1 Configure the super-VLAN and sub-VLAN.

Configure sub-VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

Add XGE 0/0/1 and XGE 0/0/2 to sub-VLAN 2.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
[Quidway-XGigabitEthernet0/0/1] port default vlan 2
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 2
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure sub-VLAN 3.

```
<Quidway> system-view
[Quidway] vlan 3
[Quidway-vlan3] quit
```

Add XGE0/0/3 and XGE0/0/4 to sub-VLAN 3.

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] port link-type access
[Quidway-XGigabitEthernet0/0/3] port default vlan 3
[Quidway-XGigabitEthernet0/0/3] quit
[Quidway] interface xgigabitethernet 0/0/4
[Quidway-XGigabitEthernet0/0/4] port link-type access
[Quidway-XGigabitEthernet0/0/4] port default vlan 3
[Quidway-XGigabitEthernet0/0/4] quit
```

Configure super-VLAN 4 and add sub-VLAN 2 to super-VLAN 4.

```
[Quidway] vlan 4
[Quidway-vlan4] aggregate-vlan
[Quidway-vlan4] access-vlan 2
[Quidway-vlan4] access-vlan 3
[Quidway-vlan4] quit
```

Step 2 Create and configure VLANIF 4.

Create VLANIF 4.

```
[Quidway] interface vlanif 4
```

Assign an IP address to VLANIF 4.

```
[Quidway-Vlanif4] ip address 10.10.10.1 24
```

Step 3 Enable inter-VLAN proxy ARP on VLANIF 4.

```
[Quidway-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
[Quidway-Vlanif4] quit
```

Step 4 Verify the configuration.

Run the **display current-configuration** command. You can view the configurations of the super-VLAN, sub-VLAN, and VLANIF interface. For query results, see the following configuration file.

Run the **display arp** command to view all the ARP entries.

```
<Quidway> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN
------------------------------------------------------------------------------
10.10.10.1      0018-2000-0083            I -         Vlanif4
10.10.10.2      00e0-fc00-0002  19        D-0         XGE0/0/1
                                          2
10.10.10.3      00e0-fc00-0003  19        D-0         XGE0/0/2
                                          2
10.10.10.4      00e0-fc00-0004  19        D-0         XGE0/0/3
                                          3
10.10.10.5      00e0-fc00-0005  19        D-0         XGE0/0/4
                                          3
------------------------------------------------------------------------------
Total:5         Dynamic:4       Static:0    Interface:1
```

----End

Configuration Files

The following lists the configuration file of the Switch.

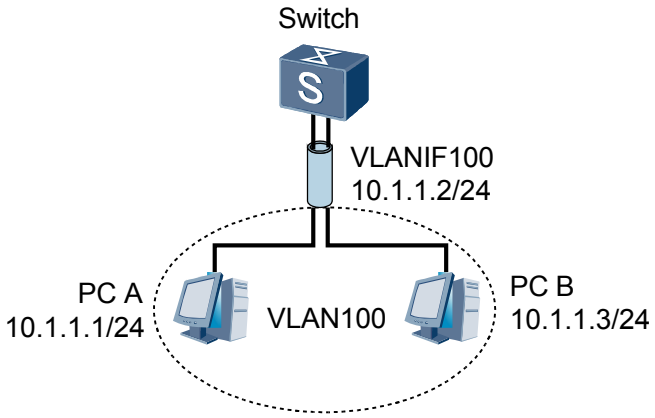
```
#
 sysname Quidway
#
 vlan batch 2 to 4
#
vlan 4
 aggregate-vlan
 access-vlan 2 to 3
#
interface Vlanif4
 ip address 10.10.10.1 255.255.255.0
 arp-proxy inter-sub-vlan-proxy enable
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface XGigabitEthernet0/0/3
 port link-type access
 port default vlan 3
#
interface XGigabitEthernet0/0/4
 port link-type access
 port default vlan 3
#
return
```

2.2.5 Example for Configuring Layer 2 Topology Detection

Networking Requirements

As shown in **Figure 2-6**, two XGE interfaces are added to VLAN 100 in default mode and the IP addresses of the two XGE interfaces are shown in the figure.

Figure 2-6 Networking diagram for configuring Layer 2 topology detection



Configuration Roadmap

The configuration roadmap is as follows:

1. Add two XGE interfaces to VLAN 100 in default mode.
2. Enable Layer 2 topology detection and view changes of ARP entries.

Data Preparation

To complete the configuration, you need the following data:

- Types and numbers of the interfaces to be added to a VLAN
- IP addresses of the VLANIF interface and the PCs

Procedure

Step 1 Create VLAN 100 and add the two XGE interfaces of the Switch to VLAN 100 in default mode.

Create VLANIF 100 and assign an IP addresses to VLANIF 100.

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] quit
[Quidway] interface vlanif 100
[Quidway-vlanif100] ip address 10.1.1.2 24
[Quidway-vlanif100] quit
```

Add the two XGE interfaces to VLAN 100 in default mode.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
```

```
[Quidway-XGigabitEthernet0/0/1] port default vlan 100
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port link-type access
[Quidway-XGigabitEthernet0/0/2] port default vlan 100
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 # Enable Layer 2 topology detection.

```
[Quidway] l2-topology detect enable
```

Step 3 Restart XGE 0/0/1 and view changes of the ARP entries and aging time.

View ARP entries on the Switch. You can find that the Switch has learnt the MAC address of the PC.

```
[Quidway] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M)  TYPE          INTERFACE   VPN-
INSTANCE
                                          VLAN
--------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900              I -           Vlanif100
10.1.1.1        00e0-c01a-4901  20          D-0           XGE0/0/1
10.1.1.3        00e0-de24-bf04  20          D-0           XGE0/0/2
--------------------------------------------------------------------------------
Total:3         Dynamic:2       Static:0    Interface:1
```

Run the **shutdown** command and then the **undoshutdown** command on XGE 0/0/1 to view the aging time of ARP entries.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] shutdown
[Quidway-XGigabitEthernet0/0/1] undo shutdown
[Quidway-XGigabitEthernet0/0/1] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN
--------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900              I -
Vlanif100
10.1.1.3        00e0-de24-bf04  0           D-0           XGE0/0/2
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

NOTE

According to the displayed information, the ARP entry learned from XGE 0/0/1 is deleted after XGE 0/0/1 is shut down. The aging time of ARP entries learned from XGE 0/0/2 becomes 0 after XGE0/0/1 is restored and becomes Up again. When the aging time is 0, the Switch sends an ARP probe packet for updating ARP entries.

```
[Quidway-XGigabitEthernet0/0/1] display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                          VLAN
--------------------------------------------------------------------------------
10.1.1.2        00e0-c01a-4900              I -
Vlanif100
10.1.1.3        00e0-de24-bf04  20          D-0           XGE0/0/2
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

NOTE

After the ARP entry is updated, the aging time is restored to the default value, 20 minutes.

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
L2-topolgy detect enable
#
 vlan 100
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 100
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 100
#
return
```

2.3 DHCP Configuration

The DHCP technology is applicable to a variety of networks. It ensures proper IP address allocation and saves IP addresses on networks.

2.3.1 Example for Configuring a DHCP Server Based on the Global Address Pool

This section describes how to configure a global address pool to allocate IP addresses for clients when the clients and DHCP server are in the same network segment.

Networking Requirements

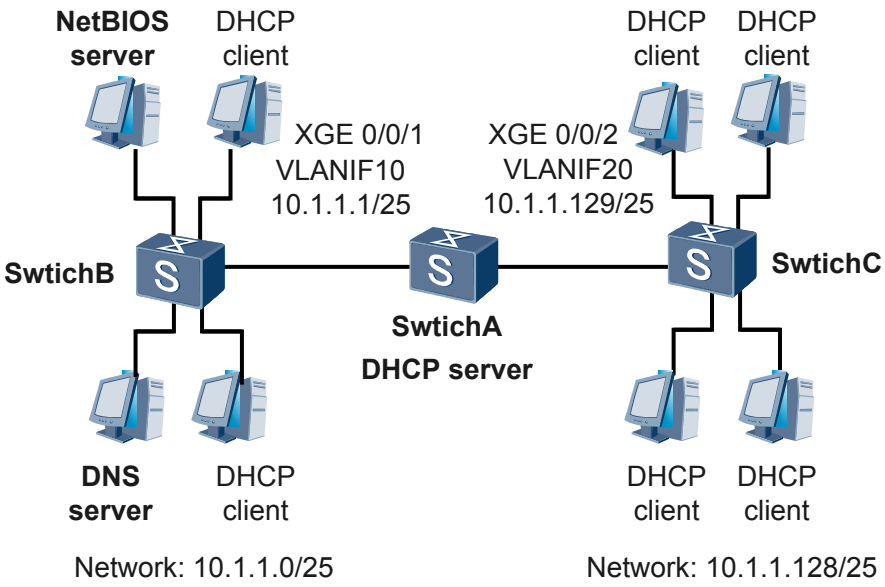
An enterprise has two offices that are in the same network segment. To reduce network construction cost, the enterprise uses one DHCP server to allocate IP addresses for the computers in the two offices.

As shown in **Figure 2-7**, SwitchA functions as the DHCP server, and SwitchB and SwitchC are user access switches. A global address pool or an interface address pool can be configured on SwitchA. This section describes how to configure a global address pool. Address pool 10.1.1.0/24 consists of two network segments: 10.1.1.0/25 and 10.1.1.128/25. The IP addresses of the VLANIF interfaces on the DHCP server are 10.1.1.1/25 and 10.1.1.129/25.

There are a few computers in network segment 10.1.1.0/25 and the computer locations are fixed. The lease of an IP address in 10.1.1.0/25 is 10 days, the DNS address is 10.1.1.2, no NetBIOS address is set, and the IP address of the egress gateway is 10.1.1.126.

There are many computers in network segment 10.1.1.128/25 and the computers are often moved from one place to another. The lease of an IP address in 10.1.1.128/25 is 2 days, the DNS address is 10.1.1.2, the NetBIOS address is 10.1.1.4, and the IP address of the egress gateway is 10.1.1.254.

Figure 2-7 Networking diagram for configuring the DHCP server based on the global address pool



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the DHCP server function on SwitchA.
2. Create a global address pool on SwitchA and set the attributes of the address pool, including the range of the address pool, egress gateway, NetBIOS address, and address lease.
3. Configure VLANIF interfaces to use the global address pool to allocate IP addresses.

Data Preparation

To complete the configuration, you need the following data:

Number and range of the global address pool on SwitchA

NOTE

The following configurations are performed on SwitchA.

Procedure

Step 1 Enable DHCP.

```
<Quidway> system-view
[Quidway] dhcp enable
```

Step 2 Create address pools and set the attributes of the address pools.

Set the attributes of IP address pool 1, including the address pool range, DNS address, egress gateway address, and address lease.

```
[Quidway] ip pool 1
[Quidway-ip-pool-1] network 10.1.1.0 mask 255.255.255.128
[Quidway-ip-pool-1] dns-list 10.1.1.2
```

```
[Quidway-ip-pool-1] gateway-list 10.1.1.126
[Quidway-ip-pool-1] excluded-ip-address 10.1.1.2
[Quidway-ip-pool-1] excluded-ip-address 10.1.1.4
[Quidway-ip-pool-1] lease day 10
[Quidway-ip-pool-1] quit
```

Set the attributes of IP address pool 2, including the address pool range, DNS address, egress gateway address, NetBIOS address, and address lease.

```
[Quidway] ip pool 2
[Quidway-ip-pool-2] network 10.1.1.128 mask 255.255.255.128
[Quidway-ip-pool-2] dns-list 10.1.1.2
[Quidway-ip-pool-2] nbns-list 10.1.1.4
[Quidway-ip-pool-2] gateway-list 10.1.1.254
[Quidway-ip-pool-2] lease day 2
[Quidway-ip-pool-2] quit
```

Step 3 Set the address allocation mode on the VLANIF interfaces.

Add XGE 0/0/1 to VLAN 10 and XGE 0/0/2 to VLAN 20.

```
[Quidway] vlan batch 10 20
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 20
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 20
[Quidway-XGigabitEthernet0/0/2] quit
```

Configure the clients on VLANIF 10 to obtain IP addresses from the global address pool.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 255.255.255.128
[Quidway-Vlanif10] dhcp select global
[Quidway-Vlanif10] quit
```

Configure the clients on VLANIF 20 to obtain IP addresses from the global address pool.

```
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 10.1.1.129 255.255.255.128
[Quidway-Vlanif20] dhcp select global
[Quidway-Vlanif20] quit
```

Step 4 Verify the configuration.

Run the **display ip pool** command on the S6700, and you can view the configuration of the IP address pool.

```
[Quidway] display ip pool
  ------------------------------------------------------------------------
  Pool-name      : 2
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.254
  Mask           : 255.255.255.128
  VPN instance   : --

  ------------------------------------------------------------------------
  Pool-name      : 1
  Pool-No        : 2
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.126
  Mask           : 255.255.255.128
  VPN instance   : --


   IP address Statistic
```

```
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----End

Configuration Files

Configuration file of the SwitchA

```
#
 sysname Quidway
#
 vlan batch 10 20
#
dhcp enable
#
 ip pool 1
 ip pool 2
#
ip pool 1
 gateway-list 10.1.1.126
 network 10.1.1.0 mask 255.255.255.128
 excluded-ip-address 10.1.1.2
 excluded-ip-address 10.1.1.4
 dns-list 10.1.1.2
 lease day 10 hour 0 minute 0
#
ip pool 2
 gateway-list 10.1.1.254
 network 10.1.1.128 mask 255.255.255.128
 dns-list 10.1.1.2
 nbns-list 10.1.1.4
 lease day 5 hour 0 minute 0
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.128
 dhcp select global
#
interface Vlanif20
 ip address 10.1.1.129 255.255.255.128
 dhcp select global
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

2.3.2 Example for Configuring the DHCP Server Based on the Interface Address Pool

A DHCP server can allocate IP addresses for the clients in the same network segment by using an interface address pool.

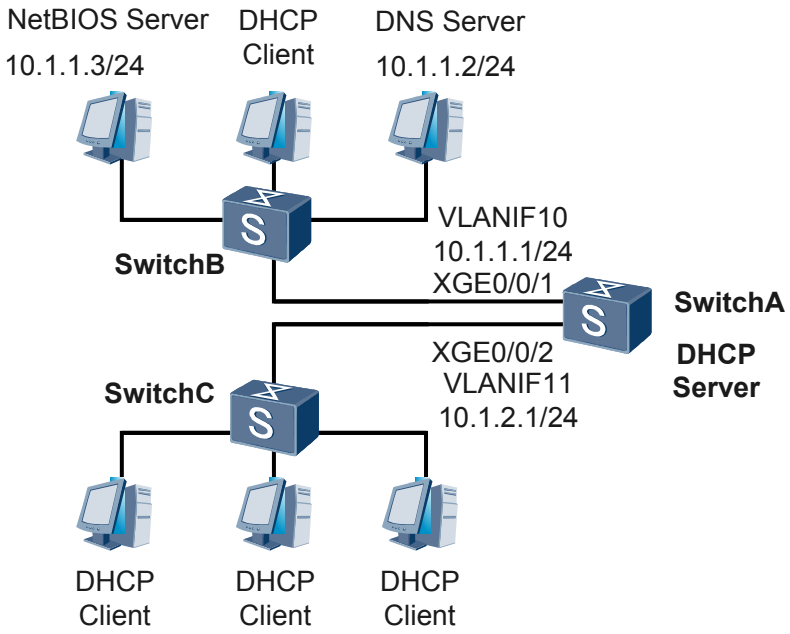
Networking Requirements

A campus has two equipment rooms, which are in different network segments. A switch needs to be configured as a DHCP server to allocate IP addresses for the computers in the two equipment rooms.

The DHCP server is connected to the access switches of the two equipment rooms, and allocates IP addresses for the computers by using two interface address pools.

As shown in **Figure 2-8**, SwitchA functions as the DHCP server, and SwitchB and SwitchC are the access switches. The two VLANIF interface address pools need to be configured on XGE 0/0/1 and XGE 0/0/2 of SwitchA.

Figure 2-8 Networking diagram for configuring a DHCP server based on a VLANIF interface address pool



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure SwitchA as a DHCP server.
2. Create VLANIF interfaces and allocate IP addresses to VLANIF interfaces to determine the range of address pools.
3. Enable the VLANIF interface address pools.
4. Set the address pool attributes, including the DNS server address, NetBIOS server address, and IP address lease.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the interfaces
- DNS server address and NetBIOS server address
- Address lease in the address pool

Procedure

Step 1 Enable DHCP.

```
<Quidway> system-view
[Quidway] dhcp enable
```

Step 2 Add interfaces to VLANs.

Add XGE 0/0/1 to VLAN 10.

```
[Quidway] vlan batch 10 to 11
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
```

Add XGE 0/0/2 to VLAN 11.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 11
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 11
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 3 Allocate IP addresses to VLANIF interfaces.

Allocate an IP address to VLANIF 10.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 24
[Quidway-Vlanif10] quit
```

Allocate an IP address to VLANIF 11.

```
[Quidway] interface vlanif 11
[Quidway-Vlanif11] ip address 10.1.2.1 24
[Quidway-Vlanif11] quit
```

Step 4 Enable the VLANIF interface address pool.

Configure the clients on VLANIF 10 to obtain IP addresses from the interface address pool.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcp select interface
[Quidway-Vlanif10] quit
```

Configure the clients on VLANIF 11 to obtain IP addresses from the interface address pool.

```
[Quidway] interface vlanif 11
[Quidway-Vlanif11] dhcp select interface
[Quidway-Vlanif11] quit
```

Step 5 Configure the DNS service and NetBIOS services of the address pool.

Configure the DNS service and NetBIOS service of VLANIF 10 address pool.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcp server domain-name huawei.com
[Quidway-Vlanif10] dhcp server dns-list 10.1.1.2
[Quidway-Vlanif10] dhcp server nbns-list 10.1.1.3
[Quidway-Vlanif10] dhcp server excluded-ip-address 10.1.1.2
[Quidway-Vlanif10] dhcp server excluded-ip-address 10.1.1.3
[Quidway-Vlanif10] dhcp server netbios-type b-node
```

Step 6 Set IP address leases of IP address pools.

Set the IP address lease of VLANIF 10 address pool to 30 days.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcp server lease day 30
[Quidway-Vlanif10] quit
```

Set the IP address lease of VLANIF 11 address pool to 20 days.

```
[Quidway] interface vlanif 11
[Quidway-Vlanif11] dhcp server lease day 20
[Quidway-Vlanif11] quit
```

Step 7 Verify the configuration.

Run the **display ip pool interface** command on SwitchA to view the configuration of the interface address pool.

```
[Quidway] display ip pool interface vlanif10
  Pool-Name      : vlanif10
  Pool-No        : 0
  Lease          : 30 Days 0 Hours 0 Minutes
  Domain-name    : huawei.com
  DNS-Server0    : 10.1.1.2
  NBNS-Server0   : 10.1.1.3
  Netbios-type   : b-node
  Position       : Interface       Status           : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
         Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
     10.1.1.1       10.1.1.254   253     0   251       0         0        2
 ------------------------------------------------------------------------------
[Quidway] display ip pool interface vlanif11
  Pool-Name      : vlanif11
  Pool-No        : 1
  Lease          : 20 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-Server0    : -
  NBNS-Server0   : -
  Netbios-type   : -
  Position       : Interface       Status           : Unlocked
  Gateway-0      : 10.1.2.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
         Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
       10.1.2.1     10.1.2.254   253     0   253       0         0        0
 ------------------------------------------------------------------------------
```

----End

Configuration Files

Configuration file of SwitchA

```
#
 sysname Quidway
#
 vlan batch 10 to 11
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 dhcp server excluded-ip-address 10.1.1.2 10.1.1.3
 dhcp server dns-list 10.1.1.2
 dhcp server netbios-type b-node
```

```
 dhcp server nbns-list 10.1.1.3
 dhcp server lease day 30 hour 0 minute 0
 dhcp server domain-name huawei.com
#
interface Vlanif11
 ip address 10.1.2.1 255.255.255.0
 dhcp select interface
 dhcp server lease day 20 hour 0 minute 0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
return
```

2.3.3 Example for Configuring a DHCP Relay Agent

When the DHCP server and DHCP clients are in different network segments, a DHCP relay agent is required.

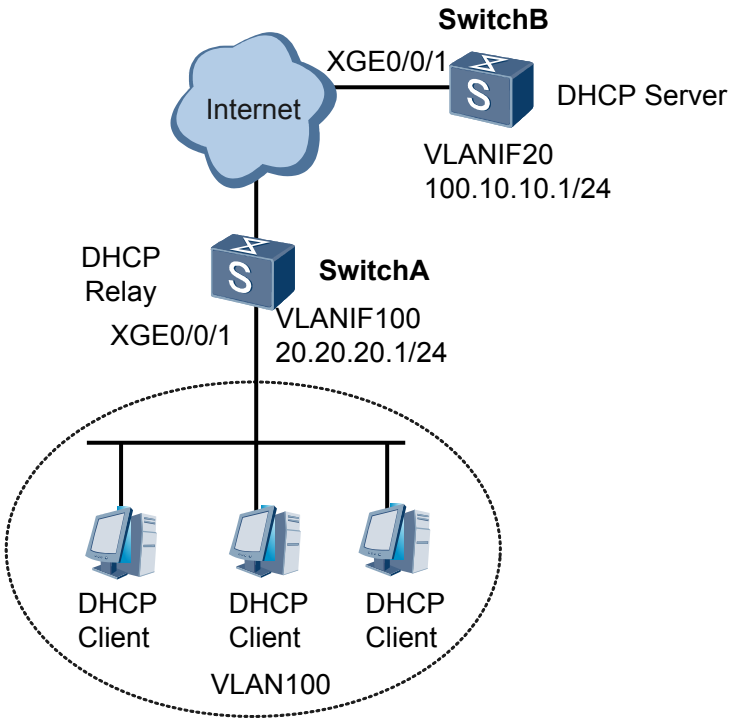
Networking Requirements

An enterprise has multiple offices, which are distributed in different office buildings. The offices in a building belong to the same local area network (LAN), and the buildings belong to different LANs. The enterprise uses a DHCP server to allocate IP addresses to all clients.

As shown in **Figure 2-9**, the DHCP clients are in the network segment 20.20.20.0/24 and the DHCP server is in the network segment 100.10.10.0/24. A Switch enabled with DHCP relay is required between the clients and server. By using the DHCP relay agent, the DHCP clients can obtain IP addresses from the DHCP server.

The DHCP server and the clients are in different network segments, and an interface-based address pool cannot allocate IP addresses to the clients in different network segments. A global address pool in the network segment 20.20.20.0/24 is required, and the DHCP server must have a reachable route to the network segment 20.20.20.0/24.

Figure 2-9 DHCP relay agent networking diagram



Configuration Roadmap

Configure SwitchA as a DHCP relay agent. The configuration roadmap is as follows:

1. Configure a DHCP server group on SwitchA and add SwitchB to the DHCP server group.
2. Enable DHCP relay on VLANIF 100.
3. Bind the DHCP server group to VLANIF 100 and specify the DHCP server for the DHCP relay agent.

Configure SwitchB as the DHCP server. The configuration roadmap is as follows:

1. Configure a reachable route from the DHCP server to XGE 0/0/1 of the DHCP relay agent.
2. Enable the DHCP function on the server. Configure the clients connected to XGE 0/0/1 of the server to obtain IP addresses from the global address pool.
3. Create a global address pool on the DHCP server to allocate IP addresses to clients.

Data Preparation

To complete the configuration, you need the following data:

- Name of the DHCP server group
- IP address of the DHCP server in the DHCP server group
- Number and IP address of the interface enabled with DHCP relay

Procedure

Step 1 Create a DHCP server group and add DHCP servers to the DHCP server group.

Create a DHCP server group.

```
<Quidway> system-view
[Quidway] dhcp server group dhcpgroup1
```

Add DHCP servers to the DHCP server group.

```
[Quidway-dhcp-server-group-dhcpgroup1] dhcp-server 100.10.10.1
[Quidway-dhcp-server-group-dhcpgroup1] quit
```

Step 2 Enable DHCP relay on the VLANIF interface.

Create a VLAN and add XGE 0/0/1 to the VLAN.

```
[Quidway] vlan 100
[Quidway-Vlan100] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type trunk
[Quidway-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Quidway-XGigabitEthernet0/0/1] quit
```

Enable DHCP globally, and then enable DHCP Relay on the VLANIF 100 interface.

```
[Quidway] dhcp enable
[Quidway] interface vlanif 100
[Quidway-Vlanif100] dhcp select relay
[Quidway-Vlanif100] quit
```

Step 3 Bind a VLANIF interface to a specified DHCP server group.

Assign an IP address to the VLANIF interface.

```
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ip address 20.20.20.1 24
```

Bind the VLANIF interface to a specified DHCP server group.

```
[Quidway-Vlanif100] dhcp relay server-select dhcpgroup1
[Quidway-Vlanif100] quit
```

Step 4 Configure the DHCP server.

Create a VLAN and add XGE 0/0/1 to the VLAN.

```
[Quidway] vlan 20
[Quidway-Vlan20] quit
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type trunk
[Quidway-XGigabitEthernet0/0/1] port trunk allow-pass vlan 20
[Quidway-XGigabitEthernet0/0/1] quit
```

Enable the DHCP function and configure the clients connected to VLANIF 20 to obtain IP addresses from the global address pool.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ip address 100.10.10.1 24
[Quidway-Vlanif20] dhcp select global
[Quidway-Vlanif20] quit
```

Configure an IP address pool 20.20.20.0/24 on the DHCP server and configure a static route from the DHCP server to the Switch. Ensure that the route between the DHCP server and network segment 20.20.20.0/24 is reachable.

```
[Quidway] ip pool 1
[Quidway-ip-pool-1] network 20.20.20.0 mask 24
[Quidway-ip-pool-1] quit
```

Configure a static route from the address pool to the DHCP relay agent to ensure that the DHCP server has a reachable route to the network segment 20.20.20.0/24.(The configuration procedure is not provided here.)

Step 5 Verify the configuration.

Run the **display dhcp relay** command on SwitchA to view the DHCP relay configuration on the interface.

```
[Quidway] display dhcp relay interface vlanif100
 DHCP relay agent running information of interface Vlanif100 :
 Server group name      : dhcpgroup1
 Gateway address in use : 100.10.10.1
```

Run the **display ip pool** command on SwitchB to view the address pool configuration.

```
[Quidway] display ip pool
   ------------------------------------------------------------------------
  Pool-Name      : 1
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : -
  Mask           : 255.255.255.0
  Vpn instance   : --
 IP address Statistic
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----End

Configuration Files

Configuration file of SwitchA

```
#
 sysname Quidway
#
 vlan 100
#
 dhcp enable
#
dhcp server group dhcpgroup1
 dhcp-server 100.10.10.1
#
interface Vlanif100
 ip address 20.20.20.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select dhcpgroup1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

Configuration file of SwitchB

```
#
 sysname Quidway
#
 vlan batch 20
#
dhcp enable
 #
```

```
ip pool 1
 network 20.20.20.0 mask 255.255.255.0
 #
interface Vlanif20
 ip address 100.10.10.1 255.255.255.0
 dhcp select global
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

2.4 DHCPv6 Configuration

Currently, the S6700 can function as only the DHCP relay agent on IPv6 networks. This document describes how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay.

2.4.1 Example for Configuring DHCPv6 Relay

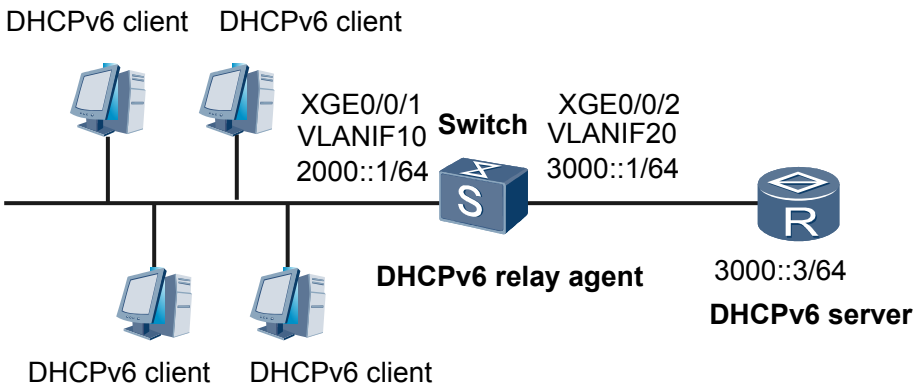
This section provides a configuration example of DHCPv6 relay.

Networking Requirements

As shown in **Figure 2-10**, the DHCPv6 client address is 2000::/64 and the DHCPv6 server address is 3000::3/64. The DHCPv6 client and the DHCPv6 server are on different links; therefore, a DHCPv6 relay agent is required to forward DHCPv6 messages.

It is required that the Switch should function as the DHCPv6 relay agent to forward DHCPv6 messages exchanged between the DHCPv6 client and the DHCPv6 server. In addition, the Switch functions as the gateway device of the network at 2000::/64. By specifying the M flag bit and O flag bit in RA messages, hosts on the network are enabled to obtain IPv6 addresses and other network configuration parameters through DHCPv6.

Figure 2-10 Networking for configuring DHCPv6 relay



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP.
2. Create VLANIF interfaces and set IPv6 addresses of the VLANIF interfaces.
3. Enable the DHCPv6 relay function and set the DHCPv6 server address.
4. Configure the Switch as the gateway.

Data Preparation

To complete the configuration, you need the following data:

- IPv6 addresses of the interfaces
- IP address of the DHCPv6 server

Procedure

Step 1 Enable DHCP.

```
<Quidway> system-view
[Quidway] dhcp enable
```

Step 2 Add interfaces to VLANs.

Add XGigabitEthernet0/0/1 to VLAN 10.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
```

Add XGigabitEthernet0/0/2 to VLAN 20.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 20
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 20
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 3 Set IPv6 addresses of VLANIF interfaces.

Enable the IPv6 packet forwarding function.

```
[Quidway] ipv6
```

Set the IPv6 address of VLANIF 10.

```
[Quidway] vlan batch 10 20
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ipv6 enable
[Quidway-Vlanif10] ipv6 address 2000::1 64
[Quidway-Vlanif10] quit
```

Set the IPv6 address of VLANIF 20.

```
[Quidway] interface vlanif 20
[Quidway-Vlanif20] ipv6 enable
[Quidway-Vlanif20] ipv6 address 3000::1 64
[Quidway-Vlanif20] quit
```

Step 4 Enable the DHCPv6 relay function.

Enable the DHCPv6 relay function on VLANIF 10 and set the IP address of the DHCPv6 server.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] dhcpv6 relay destination 3000::3
```

Step 5 Configure the Switch as the gateway.

Configure the Switch to send RA messages and configure M and O flag bits.

```
[Quidway-Vlanif10] undo ipv6 nd ra halt
[Quidway-Vlanif10] ipv6 nd autoconfig managed-address-flag
[Quidway-Vlanif10] ipv6 nd autoconfig other-flag
[Quidway-Vlanif10] quit
```

Step 6 Verify the configuration.

Run the **display dhcpv6 relay** command on the Switch, and you can view the configuration of DHCPv6 relay.

```
[Quidway] display dhcpv6 relay
 Interface    Mode    Destination
------------------------------------------------------------------
Vlanif10     Relay   3000::3
------------------------------------------------------------------
```

Run the **display dhcpv6 relay statistics** on the Switch, and you can view the statistics about DHCP messages passing through the DHCPv6 relay agent.

```
[Quidway] display dhcpv6 relay statistics
MessageType              Receive          Send             Error
 Solicit                  0                0                0
 Advertise                0                0                0
 Request                  0                0                0
 Confirm                  0                0                0
 Renew                    0                0                0
 Rebind                   0                0                0
 Reply                    0                0                0
 Release                  0                0                0
 Decline                  0                0                0
 Reconfigure              0                0                0
 Information-request      0                0                0
 Relay-forward            0                0                0
 Relay-reply              0                0                0
 UnknownType              0                0                0
```

----End

Configuration Files

Configuration file of the Switch

```
#
 sysname Quidway
#
 vlan batch 10 20
#
 ipv6
#
dhcp enable
#
interface Vlanif10
 ipv6 enable
 ipv6 address 2000::1/64
 undo ipv6 nd ra halt
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 dhcpv6 relay destination 3000::3
#
interface Vlanif20
 ipv6 enable
 ipv6 address 3000::1/64
#
interface XGigabitEthernet0/0/1
```

```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

2.5 IP Performance Configuration

This chapter describes the basic concepts of IP performance, and provides configuration procedures and examples of IP performance.

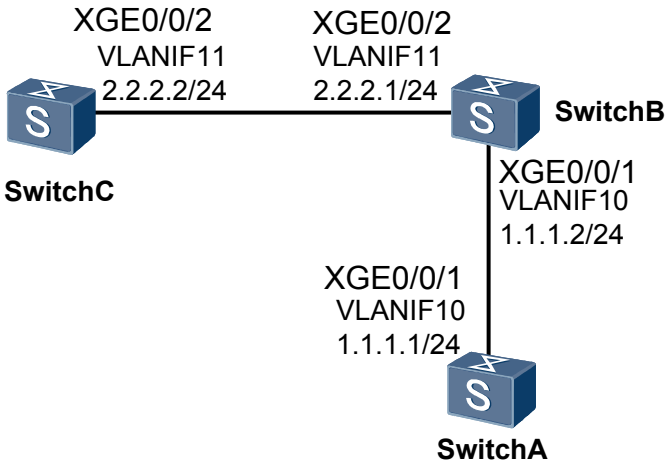
2.5.1 Example for Disabling the Sending of ICMP Host Unreachable Packets

This section provides a configuration example of disabling the sending of ICMP host unreachable packets.

Networking Requirements

As shown in **Figure 2-11**, to limit the sending of ICMP redirection packets, Switch A, Switch B, and Switch C are required and these devices are connected through their XGigabitEthernet interfaces.

Figure 2-11 Networking diagram for disabling the sending of ICMP host unreachable packets



Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to interfaces on Switches.
2. Configure static routes to indirectly connected devices.
3. Enable the sending of ICMP host unreachable packets in the system view.

4. Enable the sending of ICMP host unreachable packets in the interface view.

   NOTE

   By default, the sending of ICMP host unreachable packets is enabled on the system view and on the interface view. If the configuration is not changed, you can skip this configuration.

Data Preparation

To complete the configuration, you need the following data:

- Static routes to indirectly connected devices
- IP address of the interface

Procedure

Step 1 Configure Switch A.

Assign an IP address to VLANIF 10.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-Vlan10] quit
[SwitchA] interface xgigabitethernet0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid tagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 1.1.1.1 24
[SwitchA-Vlanif10] quit
```

Configure a static route on Switch A.

```
[SwitchA] ip route-static 2.2.2.0 24 1.1.1.2
```

Step 2 Configure Switch B.

Assign an IP address to VLANIF 10 on Switch B and disable the sending of ICMP host unreachable packets.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] icmp host-unreachable send
[SwitchB] vlan 10
[SwitchB-Vlan10] quit
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid tagged vlan 10
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 1.1.1.2 24
[SwitchB-Vlanif10] quit
[SwitchB] vlan 11
[SwitchB-Vlan11] quit
[SwitchB] interface xgigabitethernet0/0/2
[SwitchB-XGigabitEthernet0/0/2] port hybrid tagged vlan 11
[SwitchB-XGigabitEthernet0/0/2] quit
[SwitchB] interface vlanif 11
[SwitchB-Vlanif11] ip address 2.2.2.1 24
[SwitchB-Vlanif11] icmp host-unreachable send
[SwitchB-Vlanif11] quit
```

Step 3 Configure Switch C.

Assign an IP address to VLANIF 11 on Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
```

```
[SwitchC] vlan 11
[SwitchC-Vlan11] quit
[SwitchC] interface xgigabitethernet0/0/2
[SwitchC-XGigabitEthernet0/0/2] port hybrid tagged vlan 11
[SwitchC-XGigabitEthernet0/0/2] quit
[SwitchC] interface vlanif 11
[SwitchC-Vlanif11] ip address 2.2.2.2 24
[SwitchC-Vlanif11] quit
```

Step 4 Verify the configuration.

Debug ICMP packets on Switch A.

```
<SwitchA> debugging ip icmp
<SwitchA> terminal monitor
<SwitchA> terminal debugging
```

Run the **ping 2.2.2.3** command on Switch A. According to the received packet captured by the tester on Switch A, Switch B sends host unreachable packets.

```
[SwitchA] ping 2.2.2.3
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan 10
#
interface vlanif 10
 ip address 1.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 10 to 11
#
interface vlanif 10
 ip address 1.1.1.2 255.255.255.0
#
interface vlanif 11
 ip address 2.2.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 11
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan 11
#
```

```
interface vlanif 11
 ip address 2.2.2.2 255.255.255.0
 #
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 11
#
return
```

2.6 DHCP Policy VLAN Configuration

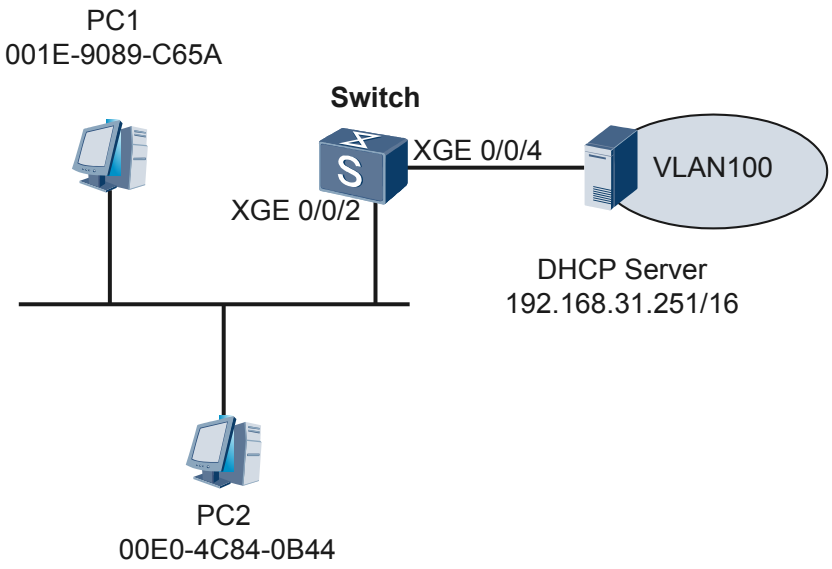
This chapter describes the concept, operating mode, and configuration of Dynamic Host Configuration Protocol (DHCP) policy Virtual Local Area Network (VLAN), and provides configuration examples.

2.6.1 Example for Configuring DHCP Policy VLAN Based on MAC Addresses

Networking Requirements

As shown in **Figure 2-12**, on the S6700, XGE 0/0/2 connects to PC1 and PC2 that access the network for the first time; XGE 0/0/4 connects to the DHCP server that belongs to VLAN 100. The MAC address of PC1 is 001E-9089-C65A; the MAC address of PC2 is 00E0-4C84-0B44.

Figure 2-12 Networking for configuring DHCP policy VLAN based on MAC addresses



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP globally.
2. Determine to which VLAN the DHCP server belongs.

3. Configure DHCP policy VLAN based on MAC addresses.

Data Preparation

To complete the configuration, you need the following data:

- MAC address of the newly added host
- Default VLAN ID of the interfaces on the S6700

Configuration Procedure

1. Configure the S6700.

   # Enable DHCP globally. Configure XGE 0/0/2 and XGE 0/0/4 on the S6700 as a hybrid interface, and configure frames from VLAN 100 to pass through XGE 0/0/2 in untagged mode.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 2
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 2 to 100
[Quidway-XGigabitEthernet0/0/2] quit
[Quidway] interface xgigabitethernet 0/0/4
[Quidway-XGigabitEthernet0/0/4] port hybrid pvid vlan 100
[Quidway-XGigabitEthernet0/0/4] port hybrid untagged vlan 100
[Quidway-XGigabitEthernet0/0/4] quit
```

   # Configure DHCP policy VLAN based on MAC addresses.

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] dhcp policy-vlan mac-address 001E-9089-C65A priority 5
[Quidway-vlan100] dhcp policy-vlan mac-address 00E0-4C84-0B44 priority 5
[Quidway-vlan100] quit
```

2. Verify the configuration.

   # After PC1 and PC2 go online and obtain IP addresses, ping the DHCP server from PC1 and PC2. The ping operations are successful.

```
C:\>ping 192.168.31.251

Pinging 192.168.31.251 with 32 bytes of data:

Reply from 192.168.31.251: bytes=32 time=126ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255
Reply from 192.168.31.251: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.31.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 126ms, Average = 33ms
```

Configuration Files

The following lists the configuration file of the S6700.

```
#
dhcp enable
interface XGigabitEthernet0/0/2
  port hybrid pvid vlan 2
 port hybrid untagged vlan 2 to 100
interface XGigabitEthernet0/0/4
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
```

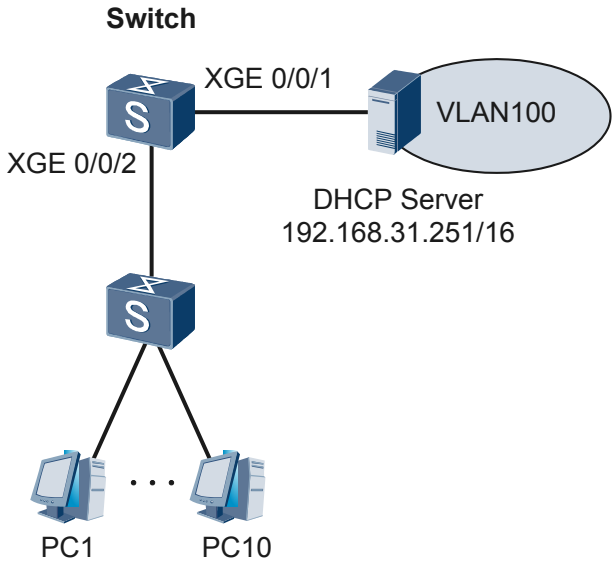
```
#
vlan 100
 dhcp policy-vlan mac-address 001e-9089-c65a priority 5
 dhcp policy-vlan mac-address 00e0-4c84-0b44 priority 5
#
return
```

2.6.2 Example for Configuring DHCP Policy VLAN Based on Interfaces

Networking Requirements

As shown in **Figure 2-13**, on the S6700, XGE 0/0/2 connects to an access switch; XGE 0/0/1 connects to the DHCP server that belongs to VLAN 100; the access switch connects to 10 hosts.

Figure 2-13 Networking for configuring DHCP policy VLAN based on interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP globally.
2. Determine to which VLAN the DHCP server belongs.
3. Configure DHCP policy VLAN based on interfaces.

Data Preparation

To complete the configuration, you need the following data:

- Number of the S6700 interface that connects to the downstream access switch
- Default VLAN ID of the interfaces on the S6700

Configuration Procedure

1. Configure the S6700.

   # Enable DHCP globally. Configure XGE 0/0/1 and XGE 0/0/2 on the S6700 as hybrid interfaces, and configure frames from VLAN 100 to pass through XGE 0/0/2 in untagged mode.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10 to 100
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 20
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 20 to 100
[Quidway-XGigabitEthernet0/0/2] quit
```

2. # Configure DHCP policy VLAN based on interfaces.

```
<Quidway> system-view
[Quidway] vlan 100
[Quidway-vlan100] dhcp policy-vlan port xgigabitethernet 0/0/2 priority 5
```

Configuration Files

The following lists the configuration file of the S6700.

```
#
dhcp enable
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10 to 100
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20 to 100
#
vlan 100
 dhcp policy-vlan port XGigabitEthernet 0/0/2 priority 5
#
return
```

2.7 DNS Configuration

By configuring the Domain Name System (DNS), you can enable network devices to communicate with other through their domain names.

2.7.1 Example for Configuring DNS

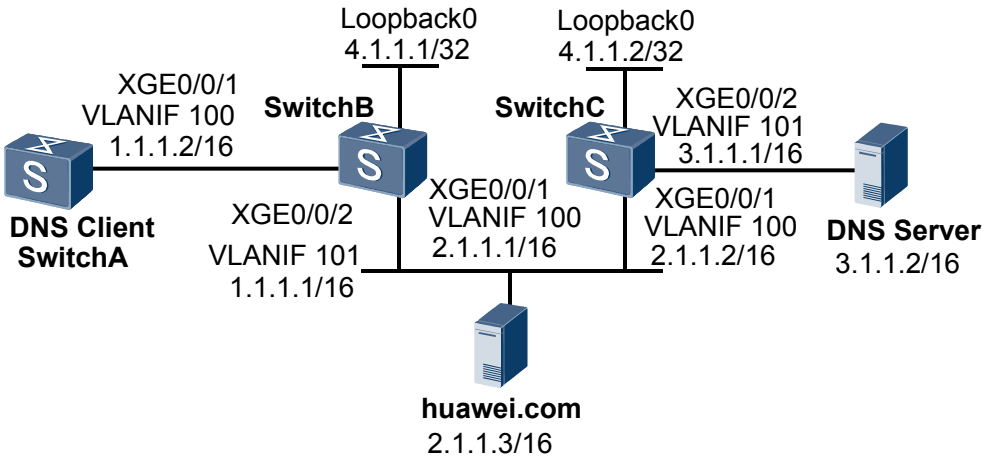
This section provides a configuration example of DNS.

Networking Requirements

As shown in **Figure 2-14**, Switch A acts as a DNS client, being required to access the host 2.1.1.3/16 by using the domain name huawei.com. You need to configure domain name suffixes "com" and "net".

On Switch A, configure static DNS entries of Switch B and Switch C so that Switch A can communicate with them by using domain names.

Figure 2-14 Networking diagram of DNS



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure static DNS entries.
2. Enable DNS resolution.
3. Configure an IP address for the DNS server.
4. Configure suffixes of domain names.

Data Preparation

To complete the configuration, you need the following data:

- Domain names of Switch B and Switch C
- IP address of the DNS server
- Suffixes of domain names

Procedure

Step 1 Configure Switch A.

Configure static DNS entries.

```
<SwitchA> system-view
[SwitchA] ip host SwitchB 4.1.1.1
[SwitchA] ip host SwitchC 4.1.1.2
```

Enable DNS resolution.

```
[SwitchA] dns resolve
```

Configure an IP address for the DNS server.

```
[SwitchA] dns server 3.1.1.2
```

Configure a domain name suffix "net".

```
[SwitchA] dns domain net
```

Configure a domain name suffix "com".

```
[SwitchA] dns domain com
[SwitchA] quit
```

NOTE

To complete DNS resolution, configuring routes from Switch A to the DNS server is mandatory. For procedures for configuring routes, refer to the Quidway S6700 Series Ethernet Switches *Configuration Guide - IP Routing*.

Step 2 Verify the configuration.

Run the **ping huawei.com** command on Switch A to ping the IP address 2.1.1.3. The ping succeeds.

```
<SwitchA> ping huawei.com
Trying DNS server (3.1.1.2)
  PING huawei.com (2.1.1.3): 56  data bytes, press CTRL_C to break
    Reply from 2.1.1.3: bytes=56 Sequence=1 ttl=126 time=6 ms
    Reply from 2.1.1.3: bytes=56 Sequence=2 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=3 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=4 ttl=126 time=4 ms
    Reply from 2.1.1.3: bytes=56 Sequence=5 ttl=126 time=4 ms

  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

Run the **display ip host** command on Switch A to view static DNS entries, including mappings between host names and IP addresses.

```
<SwitchA> display ip host
Host                 Age        Flags  Address
SwitchB              0          static 4.1.1.1
SwitchC              0          static 4.1.1.2
```

Run the **display dns dynamic-host** command on Switch A to view dynamic DNS entries in the domain name cache.

```
<SwitchA> display dns dynamic-host
No  Domain-name           IpAddress            TTL      Alias
1   huawei.com            2.1.1.3              3579
```

NOTE

TTL value in the above display indicates the lifetime of an entry. It is in seconds.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 100
#
 ip host SwitchB 4.1.1.1
 ip host SwitchC 4.1.1.2
#
 dns resolve
 dns server 3.1.1.2
 dns domain net
 dns domain com
```

```
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ip address 1.1.1.2 255.255.0.0
#
rip 1
 network 1.0.0.0
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 100 101
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface LoopBack0
 ip address 4.1.1.1 255.255.255.255
#
interface vlanif100
 ip address 2.1.1.1 255.255.0.0
#
interface vlanif101
 ip address 1.1.1.1 255.255.0.0
#
rip 1
 network 2.0.0.0
 network 1.0.0.0
 network 4.0.0.0
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 100 101
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface LoopBack0
 ip address 4.1.1.2 255.255.255.255
#
interface vlanif100
 ip address 2.1.1.2 255.255.0.0
#
interface vlanif101
 ip address 3.1.1.1 255.255.0.0
#
rip 1
 network 2.0.0.0
 network 3.0.0.0
network 4.0.0.0
```

```
#
return
```

2.8 Basic Configurations of IPv6

This chapter describes the basic concept and configurations of IPv6.

2.8.1 Example for Setting an IPv6 Address for an Interface

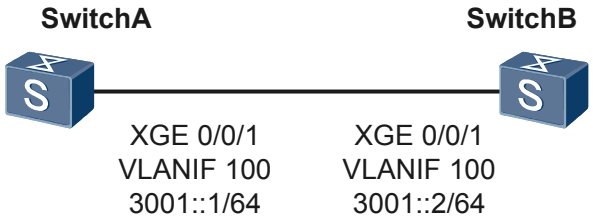
This section provides a configuration example of IPv6 address for an interface.

Networking Requirements

As shown in **Figure 2-15**, two Switches are connected through XGE 0/0/1. The XGE 0/0/1 interfaces of Switch A and Switch B correspond to their VLANIF 100 interfaces. You need to set IPv6 global unicast addresses for the VLANIF 100 interfaces and check the Layer 3 interconnection between them.

The IPv6 global unicast addresses for the interfaces are 3001::1/64 and 3001::2/64.

Figure 2-15 Networking diagram for setting IPv6 addresses



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the IPv6 forwarding capability on the Switch.
2. Set IPv6 global unicast addresses for the interfaces.

Data Preparation

To complete the configuration, you need the following data.

- Global unicast address of an interface

Procedure

Step 1 Enable the IPv6 forwarding capability on the Switch.

Configure Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
```

Configure Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
```

Step 2 Configure the IPv6 global unicast address for the interfaces.

Configure Switch A.

```
[SwitchA] vlan 100
[SwitchA-Vlan100] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ipv6 enable
[SwitchA-Vlanif100] ipv6 address 3001::1/64
[SwitchA-Vlanif100] quit
```

Configure Switch B.

```
[SwitchB] vlan 100
[SwitchB-Vlan100] quit
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ipv6 enable
[SwitchB-Vlanif100] ipv6 address 3001::2/64
[SwitchB-Vlanif100] quit
```

Step 3 Verify the configuration.

If the configuration succeeds, you can view the configured global unicast addresses. The status of the interface and the IPv6 protocol are Up.

Display information about the interface on Switch A.

```
[SwitchA] display ipv6 interface vlanif 100
Vlanif100 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::218:20FF:FE00:83 [TENTATIVE]
  Global unicast address(es):
    3001::1, subnet is 3001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF00:83
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Display information about the interface on Switch B.

```
[SwitchB] display ipv6 interface vlanif 100
Vlanif100 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE33:11 [TENTATIVE]
  Global unicast address(es):
    3001::2, subnet is 3001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:2
    FF02::1:FF33:11
    FF02::2
    FF02::1
```

```
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

On Switch A, ping the link-local address of Switch B. Note that you need to use the parameter **-i** to specify the interface of the link-local address.

```
[SwitchA] ping ipv6 FE80::2E0:FCFF:FE33:11 -i vlanif 100
  PING FE80::2E0:FCFF:FE33:11 : 56  data bytes, press CTRL_C to break
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=1 hop limit=64  time = 7 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=3 hop limit=64  time = 3 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=4 hop limit=64  time = 3 ms
    Reply from FE80::2E0:FCFF:FE33:11
    bytes=56 Sequence=5 hop limit=64  time = 3 ms

  --- FE80::2E0:FCFF:FE33:11 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/7 ms
```

On Switch A, ping the IPv6 global unicast address of Switch B.

```
[SwitchA] ping ipv6 3001::2
  PING 3001::2 : 56  data bytes, press CTRL_C to break
    Reply from 3001::2
    bytes=56 Sequence=1 hop limit=64  time = 12 ms
    Reply from 3001::2
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from 3001::2
    bytes=56 Sequence=3 hop limit=64  time = 3 ms
    Reply from 3001::2
    bytes=56 Sequence=4 hop limit=64  time = 3 ms
    Reply from 3001::2
    bytes=56 Sequence=5 hop limit=64  time = 3 ms

  --- 3001::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/4/12 ms
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
ipv6
#
 vlan 100
#
interface Vlanif100
 ipv6 enable
 ipv6 address 3001::1/64
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
```

```
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
ipv6
#
 vlan 100
#
interface Vlanif100
 ipv6 enable
 ipv6 address 3001::2/64
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

2.9 IPv6 DNS Configuration

By configuring the IPv6 Domain Name System (DNS), you can enable network devices to communicate with other through their domain names.

2.9.1 Example for Configuring IPv6 DNS

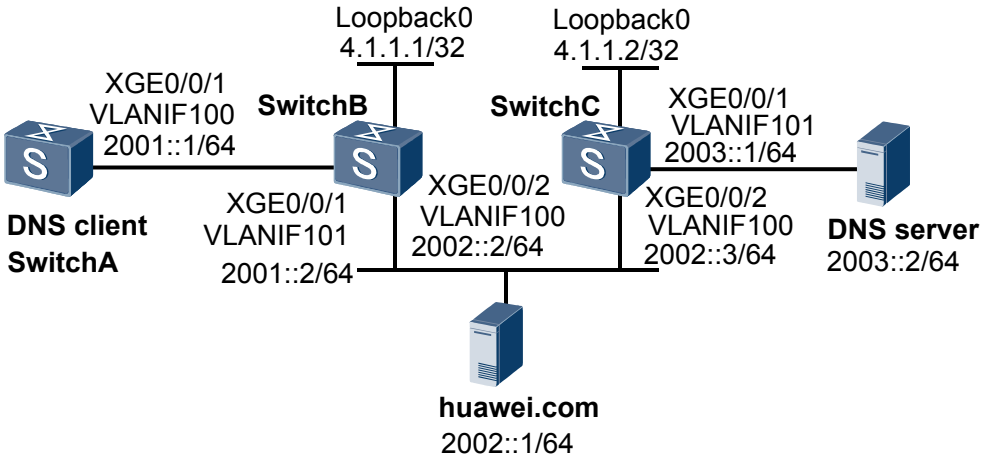
This section provides a configuration example of IPv6 DNS.

Networking Requirements

As shown in **Figure 2-16**, Switch A, functioning as the IPv6 DNS client and working jointly whose IPv6 DNS server, can access the host with the IP address as 2002::1/64 based on the domain name huawei.com.

On Switch A, the static IPv6 DNS entries of Switch B and Switch C are configured. This ensures that Switch A can manage both the routers based on the domain names Switch B and Switch C.

Figure 2-16 Networking diagram of IPv6 DNS configurations



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure static IPv6 DNS entries.
2. Enable the DNS resolution function.
3. Configure IPv6 address of the IPv6 DNS server.
4. Set the domain name suffix.

Data Preparation

To complete the configuration, you need the following data:

- Domain names of Switch B and Switch C
- IPv6 address of the IPv6 DNS server
- Domain name suffix

Procedure

Step 1 Configure Switch A.

Configure static IPv6 DNS entries.

```
<SwitchA> system-view
[SwitchA] ipv6 host RouterB 2001::2
[SwitchA] ipv6 host RouterC 2002::3
```

Enable the DNS resolution function.

```
[SwitchA] dns resolve
```

Configure the IPv6 address of the IPv6 DNS server.

```
[SwitchA] dns server ipv6 2003::2
```

Set the domain name suffix to ".net".

```
[SwitchA] dns domain net
```

Set the domain name suffix to ".com".

```
[SwitchA] dns domain com
[SwitchA] quit
```

NOTE

To resolve the domain name, you also need to configure the route from Switch A to the IPv6 DNS server. For details of how to configure the route, see Configuration example of IP static route in the Quidway S6700 Series Ethernet Switches Configuration Guide - IP Routing.

Step 2 Verify the configuration.

Run the **ping ipv6 huawei.com** command on Switch A. You can find that the Ping operation succeeds, and the destination IP address is 2002::1.

```
<SwitchA> ping ipv6 huawei.com
  Resolved Host ( huawei.com -> 2002::1)
  PING huawei.com : 56  data bytes, press CTRL_C to break
    Reply from 2002::1: bytes=56 Sequence=1 ttl=126 time=6 ms
    Reply from 2002::1: bytes=56 Sequence=2 ttl=126 time=4 ms
    Reply from 2002::1: bytes=56 Sequence=3 ttl=126 time=4 ms
    Reply from 2002::1: bytes=56 Sequence=4 ttl=126 time=4 ms
```

```
    Reply from 2002::1: bytes=56 Sequence=5 ttl=126 time=4 ms

  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

Run the **display ipv6 host** command on SwitchA. You can view the mapping relationships between the host names in static IPv6 DNS entries and the IPv6 addresses.

```
<SwitchA> display ipv6 host
Host              Age        Flags   IPv6Address (es)
SwitchB           0          static  2001::2
SwitchC           0          static  2002::3
```

Run the **display dns ipv6 dynamic-host** command on SwitchA. You can view information about dynamic IPv6 DNS entries in the dynamic cache.

```
<SwitchA> display dns ipv6 dynamic-host
No  Domain-name           Ipv6address          TTL
1   huawei.com            2002::1              3579
```

NOTE

TTL in the command output indicates the life time of the entry, in seconds.

----End

Configuration Files

- Configuration file of Switch A
- ```
  #
   sysname SwitchA
  #
  vlan batch 100
  #
   ipv6
  #
   ipv6 host SwitchB 2001::2
   ipv6 host SwitchC 2002::3
  #
   dns resolve
   dns server ipv6 2003::2
   dns domain net
   dns domain com
  #
  interface XGigabitEthernet0/0/1
   port hybrid pvid vlan 100
   port hybrid untagged vlan 100
  #
  interface vlanif100
   ipv6 enable
   ipv6 address 2001::1/64
  #
  return
  ```
- Configuration file of Switch B

  ```
  #
   sysname SwitchB
  #
  vlan batch 100 101
  #
   ipv6
  #
  interface XGigabitEthernet0/0/1
   port hybrid pvid vlan 101
   port hybrid untagged vlan 101
  ```
  ```

```
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ipv6 enable
 ipv6 address 2002::2/64
#
interface vlanif101
 ipv6 enable
 ipv6 address 2001::2/64
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 100 101
#
 ipv6
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface vlanif100
 ipv6 enable
 ipv6 address 2002::3/64
#
interface vlanif101
ipv6 enable
 ipv6 address 2003::1/64
#
return
```

2.10 IPv6 over IPv4 Tunnel Configuration

The IPv6 over IPv4 tunnel technology is developed to address the problem in the transition from IPv4 networks to IPv6 networks.

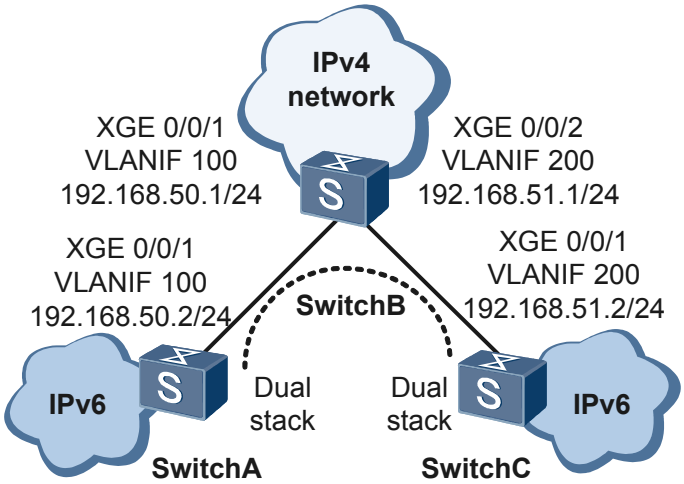
2.10.1 Example for Configuring an IPv6 over IPv4 Tunnel Manually

This section provides a configuration example of manual IPv6 over IPv4 tunnel.

Networking Requirements

As shown in **Figure 2-17**, two IPv6 networks are connected to Switch B on the IPv4 backbone network respectively through Switch A and Switch C. To enable the communication between two IPv6 networks, manually configure an IPv6 over IPv4 tunnel between Switch A and Switch C.

Figure 2-17 Networking diagram for configuring the IPv6 over IPv4 tunnel manually



Configuration Roadmap

The configuration roadmap is as follows:

1. Enabling the service loopback function on an Eth-Trunk interface.
2. Set the IP address for the VLANIF interface mapping with the physical interface.
3. Configure IPv6 addresses, source interface, and destination addresses for the tunnel interfaces.
4. Set the tunnel protocol to IPv6-IPv4.

Data Preparation

To complete the configuration, you need the following data.

- IP addresses of interfaces
- IPv6 address, source address, and destination address of the tunnel

Procedure

Step 1 Configure Switch A.

Enabling the service loopback function on an Eth-Trunk interface.

CAUTION

The interface must be idle. That is, the interface does not transmit services.

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface xgigabitethernet 0/0/3
```

```
[Quidway-XGigabitEthernet0/0/3] eth-trunk 1
[Quidway-XGigabitEthernet0/0/3] quit
```

Assign IP addresses to interfaces.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
[SwitchA] vlan 100
[SwitchA-Vlan100] quit
[SwitchA] interface xgigabitethernet0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 192.168.50.2 255.255.255.0
[SwitchA-Vlanif100] quit
```

Set the tunnel protocol to IPv6-IPv4.

```
[SwitchA] interface tunnel 0/0/1
[SwitchA-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
```

Bind the tunnel interface to the Eth-Trunk.

```
[SwitchA-Tunnel0/0/1] eth-trunk 1
```

Set IPv6 address and destination address for the tunnel interface.

```
[SwitchA-Tunnel0/0/1] ipv6 enable
[SwitchA-Tunnel0/0/1] ipv6 address 3001::1/64
[SwitchA-Tunnel0/0/1] source vlanif 100
[SwitchA-Tunnel0/0/1] destination 192.168.51.2
[SwitchA-Tunnel0/0/1] quit
```

Configure a static route.

```
[SwitchA] ip route-static 192.168.51.2 255.255.255.0 192.168.50.1
```

Step 2 Configure Switch B.

Assign IP addresses to interfaces.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
[SwitchB] vlan 100
[SwitchB-Vlan100] quit
[SwitchB] vlan 200
[SwitchB-Vlan200] quit
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet0/0/2
[SwitchB-XGigabitEthernet0/0/2] port hybrid pvid vlan 200
[SwitchB-XGigabitEthernet0/0/2] port hybrid untagged vlan 200
[SwitchB-XGigabitEthernet0/0/2] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 192.168.50.1 255.255.255.0
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] ip address 192.168.51.1 255.255.255.0
[SwitchB-Vlanif200] quit
```

Step 3 Configure Switch C.

Enabling the service loopback function on an Eth-Trunk interface.

CAUTION

The interface must be idle. That is, the interface does not transmit services.

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface xgigabitethernet0/0/1
[Quidway-XGigabitEthernet0/0/3] eth-trunk 1
[Quidway-XGigabitEthernet0/0/3] quit
```

Assign IP addresses to interfaces.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] ipv6
[SwitchC] vlan 200
[SwitchC-Vlan200] quit
[SwitchC] interface xgigabitethernet0/0/1
[SwitchC-XGigabitEthernet0/0/1] port hybrid pvid vlan 200
[SwitchC-XGigabitEthernet0/0/1] port hybrid untagged vlan 200
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface vlanif 200
[SwitchC-Vlanif200] ip address 192.168.51.2 255.255.255.0
[SwitchC-Vlanif200] quit
```

Set the tunnel protocol to IPv6-IPv4.

```
[SwitchC] interface tunnel 0/0/1
[SwitchC-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
```

Bind the tunnel interface to the Eth-Trunk.

```
[SwitchC-Tunnel0/0/1] eth-trunk 1
```

Set IPv6 address and destination address for the tunnel interface.

```
[SwitchC-Tunnel0/0/1] ipv6 enable
[SwitchC-Tunnel0/0/1] ipv6 address 3001::2/64
[SwitchC-Tunnel0/0/1] source vlanif 200
[SwitchC-Tunnel0/0/1] destination 192.168.50.2
[SwitchC-Tunnel0/0/1] quit
```

Configure a static route.

```
[SwitchC] ip route-static 192.168.50.2 255.255.255.0 192.168.51.1
```

Step 4 Verify the configuration.

On Switch C, ping the IPv4 address of VLANIF 100 of Switch A. Switch C can receive the response packet from Switch A.

```
[SwitchC] ping 192.168.50.2
  PING 192.168.50.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.50.2: bytes=56 Sequence=1 ttl=255 time=84 ms
    Reply from 192.168.50.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 192.168.50.2: bytes=56 Sequence=3 ttl=255 time=25 ms
    Reply from 192.168.50.2: bytes=56 Sequence=4 ttl=255 time=3 ms
    Reply from 192.168.50.2: bytes=56 Sequence=5 ttl=255 time=24 ms

  --- 192.168.50.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/32/84 ms
```

On Switch C, ping the IPv6 address of Tunnel 0/0/1 of Switch A. Switch C can receive the response packet from Switch A.

```
[SwitchC] ping ipv6 3001::1
  PING 3001::1 : 56  data bytes, press CTRL_C to break
    Reply from 3001::1
    bytes=56 Sequence=1 hop limit=255  time = 28 ms
    Reply from 3001::1
    bytes=56 Sequence=2 hop limit=255  time = 27 ms
    Reply from 3001::1
    bytes=56 Sequence=3 hop limit=255  time = 26 ms
    Reply from 3001::1
    bytes=56 Sequence=4 hop limit=255  time = 27 ms
    Reply from 3001::1
    bytes=56 Sequence=5 hop limit=255  time = 26 ms
  --- 3001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 26/26/28 ms
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
ipv6
#
vlan batch 100
#
interface Vlanif100
 192.168.50.2 255.255.255.0
#
interface Eth-Trunk1
 service type tunnel
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 3001::1/64
 tunnel-protocol ipv6-ipv4
 source Vlanif100
 destination 192.168.51.2
#
ip route-static 192.168.51.0 255.255.255.0 192.168.50.1
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 100 200
#
interface Vlanif100
 192.168.50.1 255.255.255.0
#
interface Vlanif200
```

```
 192.168.51.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
ipv6
#
vlan batch 200
#
interface Vlanif200
 192.168.51.2 255.255.255.0
#
interface Eth-Trunk1
 service type tunnel
#

interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 3001::2/64
 tunnel-protocol ipv6-ipv4
 source Vlanif200
 destination 192.168.50.2
#
ip route-static 192.168.50.0 255.255.255.0 192.168.51.1
#
return
```

2.10.2 Example for Configuring a 6to4 Tunnel

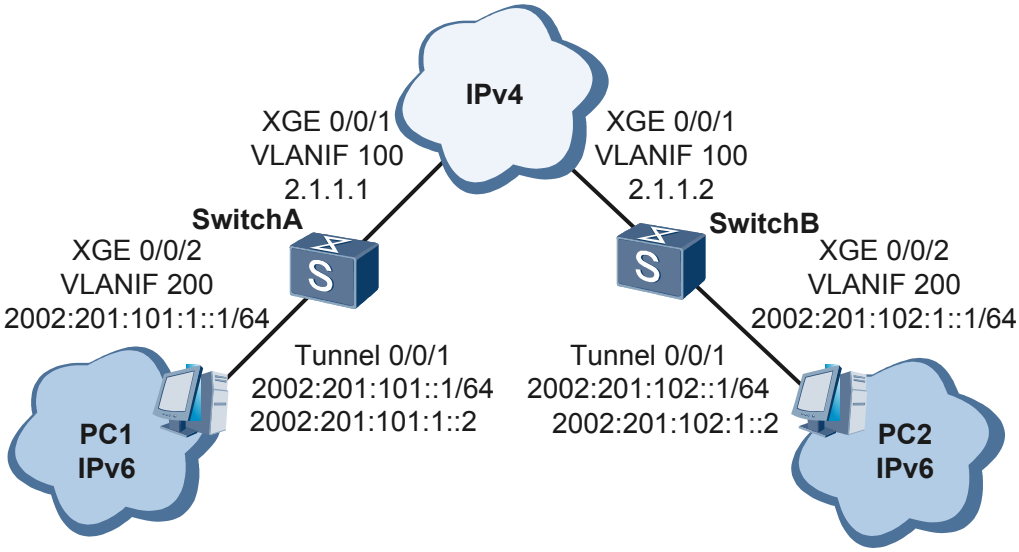
This section provides a configuration example of 6to4 tunnel.

Networking Requirements

As shown in **Figure 2-18**, Switch A and Switch B are connected to a 6to4 network and an IPv4 backbone network respectively. To enable communication between two 6to4 network hosts, you need to manually configure an 6to4 tunnel between Switch A and Switch B.

To enable communication between 6to4 networks, configure 6to4 addresses for the hosts on the 6to4 network. A 6to4 address has a 48-bit prefix, which is in the format 2002:IPv4 address. As shown in **Figure 2-18**, the IPv4 address of the interface through which Switch A is connected to the IPv4 network is 2.1.1.1. Therefore, the 6to4 address prefix of the 6to4 network where Switch A is located is 2002:0201:0101::.

Figure 2-18 Networking diagram for configuring a 6to4 tunnel



Configuration Roadmap

The configuration roadmap is as follows:

1. Enabling the service loopback function on an Eth-Trunk interface.
2. Configure the IPv4/IPv6 stack on the Switch.
3. Configure a 6to4 tunnel on the Switch.
4. Configure related routes on the Switch.

Data Preparation

To complete the configuration, you need the following data.

- IPv4 and IPv6 addresses of interfaces
- Source tunnel interface

Procedure

Step 1 # Configure Switch A.

Enabling the service loopback function on an Eth-Trunk interface.

CAUTION

The interface must be idle. That is, the interface does not transmit services.

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
```

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] eth-trunk 1
[Quidway-XGigabitEthernet0/0/3] quit
```

Configure the IPv4/IPv6 stack.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
[SwitchA] vlan batch 100 200
[SwitchA] interface xgigabitethernet0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 2.1.1.1 8
[SwitchA-Vlanif100] quit
[SwitchA] interface xgigabitethernet0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid pvid vlan 200
[SwitchA-XGigabitEthernet0/0/2] port hybrid untagged vlan 200
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] ipv6 enable
[SwitchA-Vlanif200] ipv6 address 2002:0201:0101:1::1/64
[SwitchA-Vlanif200] quit
```

Configure a 6to4 tunnel.

```
[S6700-A] interface tunnel 0/0/1
[SwitchA-Tunnel0/0/1] eth-trunk 1
[SwitchA-Tunnel0/0/1] tunnel-protocol ipv6-ipv4 6to4
[SwitchA-Tunnel0/0/1] ipv6 enable
[SwitchA-Tunnel0/0/1] ipv6 address 2002:0201:0101::1/64
[SwitchA-Tunnel0/0/1] source vlanif 100
[SwitchA-Tunnel0/0/1] quit
```

Configure a route to other 6to4 networks.

```
[SwitchA] ipv6 route-static 2002:: 16 tunnel 0/0/1
```

Step 2 # Configure Switch B.

Enabling the service loopback function on an Eth-Trunk interface.

CAUTION

The interface must be idle. That is, the interface does not transmit services.

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] eth-trunk 1
[Quidway-XGigabitEthernet0/0/3] quit
```

Configure the IPv4/IPv6 stack.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
[SwitchB] vlan batch 100 200
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
```

```
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 2.1.1.2 8
[SwitchB-Vlanif100] quit
[SwitchB] interface xgigabitethernet0/0/2
[SwitchB-XGigabitEthernet0/0/2] port hybrid pvid vlan 200
[SwitchB-XGigabitEthernet0/0/2] port hybrid untagged vlan 200
[SwitchB-XGigabitEthernet0/0/2] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] ipv6 enable
[SwitchB-Vlanif200] ipv6 address 2002:0201:0102:1::1/64
[SwitchB-Vlanif200] quit
```

Configure a 6to4 tunnel.

```
[SwitchB] interface tunnel 0/0/1
[SwitchB-Tunnel0/0/1] eth-trunk 1
[SwitchB-Tunnel0/0/1] tunnel-protocol ipv6-ipv4 6to4
[SwitchB-Tunnel0/0/1] ipv6 enable
[SwitchB-Tunnel0/0/1] ipv6 address 2002:0201:0102::1/64
[SwitchB-Tunnel0/0/1] source vlanif 100
[SwitchB-Tunnel0/0/1] quit
```

Configure a route to other 6to4 networks.

```
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0/0/1
```

NOTE

There must be a reachable route between SwitchA and SwitchB. In this example, the routing protocol needs to be configured on GigabitEthernet0/0/1 of SwitchA and SwitchB to ensure a reachable route between SwitchA and SwitchB. For the configuration procedure, see the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP Routing*.

Step 3 Verify the configuration.

View the IPv6 status of Tunnel 0/0/1 on Switch A, and you can find that the status is Up.

```
[SwitchA] display ipv6 interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::201:101 [TENTATIVE]
  Global unicast address(es):
    2002:201:101::1, subnet is 2002:201:101::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

On Switch A, ping the 6to4 address of VLANIF 200 of Switch B. Switch A can receive the response packet from Switch B.

```
[SwitchA] ping ipv6 2002:0201:0102:1::1
  PING 2002:0201:0102:1::1 : 56  data bytes, press CTRL_C to break
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=1 hop limit=255  time = 8 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=2 hop limit=255  time = 25 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=3 hop limit=255  time = 4 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=4 hop limit=255  time = 5 ms
    Reply from 2002:201:102:1::1
    bytes=56 Sequence=5 hop limit=255  time = 5 ms
```

```
  --- 2002:0201:0102:1::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 4/9/25 ms
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
ipv6
#
vlan batch 100 200
#
interface Vlanif100
 ip address 2.1.1.1 255.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002:201:101:1::1/64
#
interface Eth-Trunk1
 service type tunnel
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
XGigabitEthernet0/0/13
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 2002:201:101:1::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source vlanif100
#
ipv6 route-static 2002:: 16 Tunnel 0/0/1
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
ipv6
#
vlan batch 100 200
#
interface Vlanif100
 ip address 2.1.1.2 255.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002:201:102:1::1/64
#
interface Eth-Trunk1
 service type tunnel
#
```

```
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/1
 eth-trunk 1
 ipv6 enable
 ipv6 address 2002:201:102:1::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source vlanif100
#
ipv6 route-static 2002:: 16 Tunnel 0/0/1
#
return
```

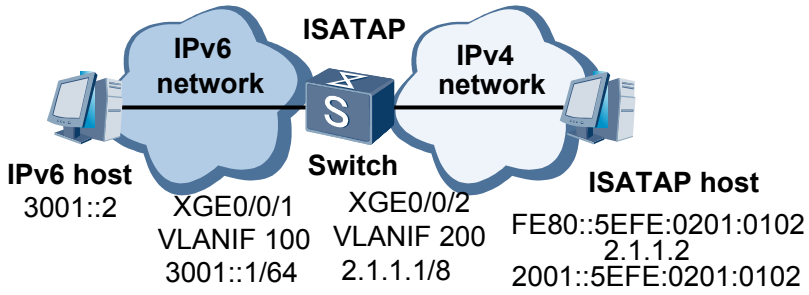
2.10.3 Example for Configuring an ISATAP Tunnel

This section provides a configuration example of ISATAP tunnel.

Network Requirements

As shown in **Figure 2-19**, an IPv6 host in the IPv4 network running the Windows XP system needs to access the IPv6 network through a border device. Both the IPv6 host and the border device support ISATAP. Then you need to set up an ISATAP tunnel between the IPv6 host and the border device.

Figure 2-19 Networking diagram of the ISATAP tunnel



Configuration Roadmap

The configuration roadmap is as follows:

1. Enabling the service loopback function on an Eth-Trunk interface.
2. Configure IPv4/IPv6 dual protocol stacks.
3. Configure an ISATAP tunnel.
4. Configure static routes from the IPv6 host to the ISATAP host.

Data Preparation

To complete the configuration, you need the following data:

- IPv4 or IPv6 addresses of interfaces
- Source interface of the tunnel
- VLAN that the physical interface of the Switch belongs to

Procedure

Step 1 Configure the ISATAP device.

Enabling the service loopback function on an Eth-Trunk interface.

CAUTION

The interface must be idle. That is, the interface does not transmit services.

```
<Quidway> system-view
[Quidway] interface eth-trunk 1
[Quidway-Eth-Trunk1] service type tunnel
[Quidway-Eth-Trunk1] quit
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] eth-trunk 1
[Quidway-XGigabitEthernet0/0/3] quit
```

Enable IPv4/IPv6 dual protocol stacks and configure an IP address for each interface.

```
<Quidway> system-view
[Quidway] ipv6
[Quidway] vlan batch 100 200
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] port hybrid pvid vlan 200
[Quidway-XGigabitEthernet0/0/2] port hybrid untagged vlan 200
[Quidway-XGigabitEthernet0/0/2] quit
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ipv6 enable
[Quidway-Vlanif100] ipv6 address 3001::1/64
[Quidway-Vlanif100] quit
[Quidway] interface vlanif 200
[Quidway-Vlanif200] ip address 2.1.1.1 255.0.0.0
[Quidway-Vlanif200] quit
```

Configure an ISATAP tunnel.

```
[Quidway] interface tunnel 0/0/2
[Quidway-Tunnel0/0/2] eth-trunk 1
[Quidway-Tunnel0/0/2] tunnel-protocol ipv6-ipv4 isatap
[Quidway-Tunnel0/0/2] ipv6 enable
[Quidway-Tunnel0/0/2] ipv6 address 2001::/64 eui-64
[Quidway-Tunnel0/0/2] source vlanif 200
[Quidway-Tunnel0/0/2] undo ipv6 nd ra halt
[Quidway-Tunnel0/0/2] quit
```

Step 2 Configure the ISATAP host.

NOTE

The ISATAP host needs to run IPv6 and needs to be enabled with the IPv6 function.

Configure a static route to the border device. (The pseudo interface number of the host is 2. You can run the **ipv6 if** command to view the interface corresponding to the automatic tunneling pseudo interface.)

```
C:\> netsh interface ipv6 isatap set router 2.1.1.1
```

Step 3 Configure the IPv6 host.

Configure a static route on the IPv6 host to the border device, so hosts in different networks can communicate through the ISATAP tunnel.

```
C:\> netsh interface ipv6 set route 2001::/64 3001::1
```

Step 4 Verify the configuration.

Check the status of the Tunnel 0/0/2 on the ISATAP device and find it is Up.

```
[Quidway] display ipv6 interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::5EFE:201:101 [TENTATIVE]
  Global unicast address(es):
    2001::5EFE:201:101, subnet is 2001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF01:101
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
```

On the ISATAP device, ping the global unicast IP address of the tunnel interface on the ISATAP host.

```
[Quidway] ping ipv6 2001::5efe:2.1.1.2
  PING 2001::5efe:2.1.1.2 : 56  data bytes, press CTRL_C to break
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=1 hop limit=64  time = 4 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=3 hop limit=64  time = 2 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 2001::5EFE:201:102
    bytes=56 Sequence=5 hop limit=64  time = 2 ms

  --- 2001::5efe:2.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/4 ms
```

On the ISATAP host, ping the global unicast IP address of the ISATAP device.

```
C:\> ping6 2001::5efe:2.1.1.1

Pinging 2001::5efe:2.1.1.1
from 2001::5efe:2.1.1.2 with 32 bytes of data:
```

```
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Reply from 2001::5efe:2.1.1.1: bytes=32 time=1ms
Ping statistics for 2001::5efe:2.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

The ISATAP host can ping through the IPv6 host.

```
C:\> ping6 3001::2

Pinging 3001::2 with 32 bytes of data:

Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms

Ping statistics for 3001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

----End

Configuration Files

The configuration file of the ISATAP device is as follows:

```
#
 sysname Quidway
#
vlan batch 100 200
#
ipv6
#
interface Vlanif100
 ipv6 enable
 ipv6 address 3001::1/64
#
interface Vlanif200
 ip address 2.1.1.1 255.0.0.0
#
interface Eth-Trunk1
 service-type tunnel
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
interface Tunnel0/0/2
 eth-trunk 1
 ipv6 enable
 ipv6 address 2001::/64 eui-64
 undo ipv6 nd ra halt
 tunnel-protocol ipv6-ipv4 isatap
 source Vlanif200
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
```

```
#
return
```

3 Configuration Guide - IP Routing

About This Chapter

This document describes the IP routing features of the S6700, including static routes. The document provides the configuration procedures and configuration examples of the IP routing features.

3.1 IP Static Route Configuration
Static routes are applicable to simple networks. Properly configuring and using static routes improve the network performance and help ensure bandwidth for important services.

3.2 RIP Configuration
RIP can advertise and receive routes to affect the selection of data forwarding paths, and can provide the network management function. RIP is applicable to small-scale networks.

3.3 RIPng Configuration
RIPng is an extension of RIP for support of IPv6.

3.4 OSPF Configuration
OSPF, which is developed by the IETF, is a link-state IGP. OSPF is widely used in access networks and MANs.

3.5 OSPFv3 Configuration
By building Open Shortest Path First Version 3 (OSPFv3) networks, you can enable OSPFv3 to discover and calculate routes in ASs. OSPFv3 is applicable to a large-scale network that consists of hundreds of routers.

3.6 IS-IS Configuration
This chapter describes the basic principle of IS-IS and procedures for configuring IS-IS, and provides configuration examples.

3.7 BGP Configuration
BGP is used between ASs to transmit routing information on large-scale and complex networks.

3.8 MBGP Configuration
MBGP is dedicated to transmitting multicast routing information across ASs.

3.9 Routing Policy Configuration
Routing policies are used to filter routes to change the path through which network traffic passes.

3.10 MCE Configuration

Generally, a Customer Edge (CE) can connect to only one Virtual Private Network (VPN). If multiple VPNs need to be divided, multiple CEs are required. The Multi-VPN-Instance CE (MCE) technology enables a CE to be connected to multiple VPNs. This isolates services between different VPNs and reduces the investment on network devices.

3.1 IP Static Route Configuration

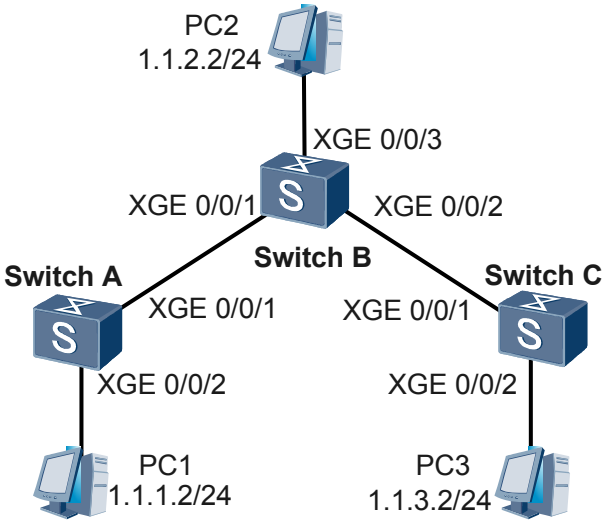
Static routes are applicable to simple networks. Properly configuring and using static routes improve the network performance and help ensure bandwidth for important services.

3.1.1 Example for Configuring IPv4 Static Routes

Networking Requirements

The PCs that belong to different network segments are connected through several switches. IPv4 static routes should be used so that any two PCs in different network segments can communicate with each other.

Figure 3-1 Networking diagram for configuring IPv4 static routes



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE0/0/1	VLANIF 10	1.1.4.1/30
SwitchA	XGE 0/0/2	VLANIF 30	1.1.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	1.1.4.2/30
SwitchB	XGE 0/0/2	VLANIF 20	1.1.4.5/30
SwitchB	XGE 0/0/3	VLANIF 40	1.1.2.1/24
SwitchC	XGE 0/0/1	VLANIF 20	1.1.4.6/30
SwitchC	XGE 0/0/2	VLANIF 50	1.1.3.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure a default IP gateway on each host.
4. Configure static routes and default routes on each switch.

Data Preparation

To complete the configuration, you need the following data:

- The IDs of the VLANs to which the interfaces belong are shown in **Figure 3-1**.
- The VLANIF interfaces and the IP addresses of the hosts are shown in **Figure 3-1**.
- The next hop address of the default route on Switch A is 1.1.4.2.
- The destination address of Switch B is 1.1.1.0, and the next hop address of the static route is 1.1.4.1.
- The destination address of Switch B is 1.1.3.0, and the next hop address of the static route is 1.1.4.6.
- The next hop address of the default route on Switch C is 1.1.4.5.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.
2. Assign an IP address to each interface.

   The configuration details are not mentioned here.
3. Configure the hosts.

   Configure default gateways of the hosts PC1, PC2, and PC3 as 1.1.1.1, 1.1.2.1, and 1.1.3.1 respectively.
4. Configure static routes.

   # Configure a default route on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
   ```

   # Configure two static routes on Switch B.

   ```
   <SwitchB> system-view
   [SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
   [SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
   ```

   # Configure a default route on Switch C.

   ```
   <SwitchC> system-view
   [SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
   ```
5. Verify the configuration.

   # Check the routing table of Switch A.

   ```
   [SwitchA] display ip routing-table
   Route Flags: R - relay, D - download to fib
   ------------------------------------------------------------------------------
   Routing Tables: Public
            Destinations : 8        Routes : 8

   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

           0.0.0.0/0   Static 60   0           RD  1.1.4.2         Vlanif10
           1.1.1.0/24  Direct 0    0           D   1.1.1.1         Vlanif30
           1.1.1.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
   ```

```
      1.1.4.0/30  Direct 0    0         D    1.1.4.1      Vlanif10
      1.1.4.1/32  Direct 0    0         D    127.0.0.1    InLoopBack
      1.1.4.2/32  Direct 0    0         D    1.1.4.2      Vlanif10
    127.0.0.0/8   Direct 0    0         D    127.0.0.1    InLoopBack0
    127.0.0.1/32  Direct 0    0         D    127.0.0.1    InLoopBack0
```

Run the **ping** command to verify the connectivity.

```
[SwitchA] ping 1.1.3.1
  PING 1.1.3.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.3.1: bytes=56 Sequence=1 ttl=254 time=62 ms
    Reply from 1.1.3.1: bytes=56 Sequence=2 ttl=254 time=63 ms
    Reply from 1.1.3.1: bytes=56 Sequence=3 ttl=254 time=63 ms
    Reply from 1.1.3.1: bytes=56 Sequence=4 ttl=254 time=62 ms
    Reply from 1.1.3.1: bytes=56 Sequence=5 ttl=254 time=62 ms

  --- 1.1.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 62/62/63 ms
```

Run the **tracert** command to verify the connectivity.

```
[SwitchA] tracert 1.1.3.1
 traceroute to  1.1.3.1(1.1.3.1), max hops: 30 ,packet length: 40
 1 1.1.4.2 31 ms  32 ms  31 ms
 2 1.1.4.6 62 ms  63 ms  62 ms
```

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 1.1.4.1 255.255.255.252
#
interface Vlanif30
 ip address 1.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 30
  port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10 20 40
#
interface Vlanif10
 ip address 1.1.4.2 255.255.255.252
#
interface Vlanif20
 ip address 1.1.4.5 255.255.255.252
#
interface Vlanif40
 ip address 1.1.2.1 255.255.255.0
#
```

```
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 40
#
ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
#
return
```

- Configuration file of Switch C

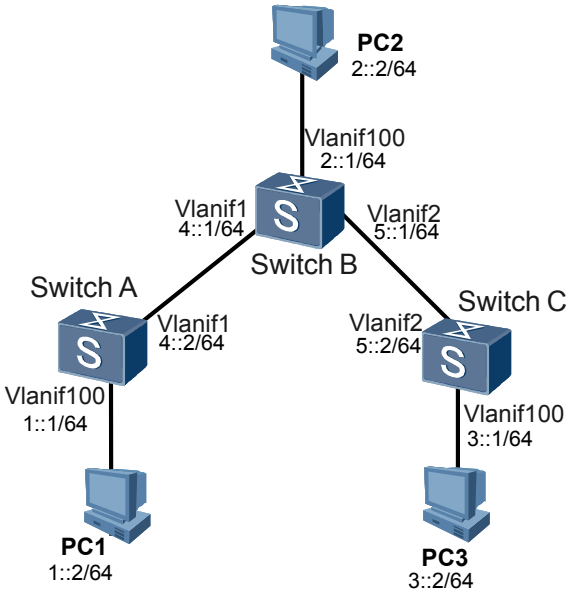
```
#
 sysname SwitchC
#
 vlan batch 20 50
#
interface Vlanif20
 ip address 1.1.4.6 255.255.255.252
#
interface Vlanif40
 ip address 1.1.3.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 50
  port hybrid untagged vlan 50
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
#
return
```

3.1.2 Example for Configuring IPv6 Static Routes

Networking Requirements

As shown in **Figure 3-2**, the mask length of all the IPv6 addresses is 64 bits. It is required that every two hosts or Switches be interconnected through IPv6 static routes.

Figure 3-2 Networking diagram for configuring IPv6 static routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IPv6 address on each Switch to make the network routable.
2. Configure the IPv6 static route and the default route to the destination address on each Switch.
3. Configure the IPv6 default gateway on each host to make any two hosts reachable.

Data Preparation

To complete the configuration, you need the following data:

- Default gateways of host PC1, host PC2, and host PC3: 1::1, 2::1, and 3::1

Configuration Procedure

1. Assign an IPv6 address to each interface. The configuration details are not mentioned here.
2. Configure IPv6 static routes.

   # Configure the IPv6 default route on Switch-A.

   ```
   [Switch-A] ipv6 route-static :: 0 4::1
   ```

   # Configure two IPv6 static routes on Switch-B.

   ```
   [Switch-B] ipv6 route-static 1:: 64 4::2
   [Switch-B] ipv6 route-static 3:: 64 5::2
   ```

   # Configure the IPv6 default route on Switch-C.

   ```
   [Switch-C] ipv6 route-static :: 0 5::1
   ```

Configuration Files

- Configuration file of Switch-A

```
#
 sysname Switch-A
#
 ipv6
#
interface Vlanif1
 ipv6 address 4::2/64
#
interface Vlanif100
 ipv6 address 1::1/64
#
#
ipv6 route-static :: 0 4::1
#
return
```

- Configuration file of Switch-B

```
#
 sysname Switch-B
#
 ipv6
#
interface Vlanif1
 ipv6 address 4::1/64
#
interface Vlanif2
 ipv6 address 5::1/64
#
interface Vlanif 100
 ipv6 address 2::1/64
#
#
ipv6 route-static 1:: 64 4::2
ipv6 route-static 3:: 64 5::2
#
return
```

- Configuration file of Switch-C

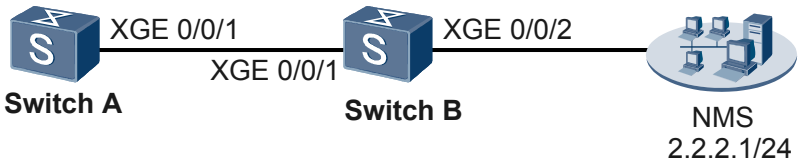
```
#
 sysname Switch-C
#
 ipv6
#
interface Vlanif2
 ipv6 address 5::2/64
#
interface Vlanif1
 ipv6 address 3::1/64
#
#
ipv6 route-static :: 0 5::1
#
return
```

3.1.3 Example for Configuring BFD for IPv4 Static Routes

Networking Requirements

As shown in **Figure 3-3**, Switch-A is connected to the network management system (NMS) through Switch-B. You can configure static routes on Switch-A so that Switch-A can communicate with the NMS. A BFD session is set up between Switch-A and Switch-B to detect link failures.

Figure 3-3 Networking diagram for configuring BFD for IPv4 static routes



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	1.1.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	1.1.1.2/24
SwitchB	XGE 0/0/2	VLANIF 20	2.2.2.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a BFD session on Switch-A and Switch-B to detect the link between Switch-A and Switch-B.
2. Configure a static route from Switch-A to the NMS and bind the static route to the BFD session.

Data Preparation

To complete the configuration, you need the following data:

- The IDs of the VLANs to which the interfaces belong are shown in **Figure 3-3**.
- The VLANIF interfaces and the IP addresses of the hosts are shown in **Figure 3-3**.
- IP address of the peer detected by BFD.
- Local and remote discriminators of the BFD session.
- Static route from Switch-A to the NMS.

Configuration Procedure

The following lists the configuration procedure of the Switch. For the configuration procedure of other devices shown in **Figure 3-3**, refer to the related configuration guides.

1. Configure the VLAN that each interface belongs to.

   The configuration details are not mentioned here.
2. Configure the IP address for each interface.

   The configuration details are not mentioned here.
3. Create a BFD session between Switch-A and Switch-B.

   # On Switch-A, create a BFD session with Switch-B.

```
<Switch-A> system-view
[Switch-A] bfd
[Switch-A-bfd] quit
[Switch-A] bfd aa bind peer-ip 1.1.1.2
[Switch-A-bfd-session-aa] discriminator local 10
[Switch-A-bfd-session-aa] discriminator remote 20
```

```
[Switch-A-bfd-session-aa] commit
[Switch-A-bfd-session-aa] quit
```

On Switch-B, create a BFD session with Switch-A.

```
<Switch-B> system-view
[Switch-B] bfd
[Switch-B-bfd] quit
[Switch-B] bfd bb bind peer-ip 1.1.1.1
[Switch-B-bfd-session-bb] discriminator local 20
[Switch-B-bfd-session-bb] discriminator remote 10
[Switch-B-bfd-session-bb] commit
[Switch-B-bfd-session-bb] quit
```

4. Configure a default static route and bind a BFD session to the default static route.

   # On Switch-A, configure a default static route to the external network and bind the default static route to a BFD session named **aa**.

   ```
   [Switch-A] ip route-static 2.2.2.1 24 1.1.1.2 track bfd-session aa
   [Switch-A] quit
   ```

5. Verify the configuration.

   # Run the **display bfd session all** command on Switch-A and Switch-B. You can view that the BFD session is set up and its status is Up.

   Take the display on Switch-A as an example.

   ```
   <Switch-A> display bfd session all
   --------------------------------------------------------------------------------
   --
   Local    Remote   PeerIPAddress     Interface Name         State          Type
   --------------------------------------------------------------------------------
   --
   10        20        1.1.1.2            --                      Up
   S_IP
   --------------------------------------------------------------------------------
   --
         Total UP/DOWN Session Number : 1/0
   ```

   # Run the **display ip routing-table** command on Switch-A. You can view that the static route exists in the routing table.

   ```
   <Switch-A> display ip routing-table
   Route Flags: R - relay, D - download to fib
   ------------------------------------------------------------------------------
   Routing Tables: Public
            Destinations : 6        Routes : 6
   Destination/Mask         Proto   Pre   Cost   Flags  NextHop        Interface
           1.1.1.0/24       Direct  0     0      D      1.1.1.1        Vlanif10
           1.1.1.1/32       Direct  0     0      D      127.0.0.1      InLoopBack0
           1.1.1.2/32       Direct  0     0      D      1.1.1.2        Vlanif10
           2.2.2.0/24       Static  60    0      RD     1.1.1.2        Vlanif10
         127.0.0.0/8        Direct  0     0      D      127.0.0.1      InLoopBack0
         127.0.0.1/32       Direct  0     0      D      127.0.0.1      InLoopBack0
   ```

   # On Switch-A, enable debugging on the terminal.

   ```
   <Switch-A> terminal monitor
   <Switch-A> terminal debugging
   ```

   # Run the **shutdown** command on VLANIF 10 of Switch-B to simulate a link fault.

   ```
   [Switch-B] interface vlanif 10
   [Switch-B-Vlanif10] shutdown
   ```

   # You can view the following debugging information on Switch-A. The information indicates that BFD detects a link fault.

   ```
   <Switch-A>
   *0.27708400 Switch-A RM/3/RMDEBUG:
    RM_USR_BFDRefreshRT_H:
    BfdSessionID  = 10
    BfdEvent       = 0X0
    USR : UsrDbID = 0X6, DestAdd = 0X0, Mask   = 0X0, NextHop = 0X1010102
   ```

```
 URT : TableID = 0X1, EntryID = 0XB, ProcID = 0X2, FLAG    = 0X8114000
```

Run the **display ip routing-table** command on Switch-A. You can view that default route 2.2.2.0/24 does not exist. This is because the BFD session is bound to the default static route. When BFD detects a fault, it rapidly notifies that the bound static route is unavailable.

```
<Switch-A> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        1.1.1.0/24  Direct  0    0           D   1.1.1.1         Vlanif10
        1.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        1.1.1.2/32  Direct  0    0           D   1.1.1.2         Vlanif10
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Run the **undo shutdown** command on VLANIF 10 of Switch-B to simulate link recovery.

```
[Switch-B-Vlanif10] undo shutdown
```

Run the **display ip routing-table** command on Switch-A. You can view that default route 2.2.2.0/24 exists. When BFD detects link recovery, it rapidly notifies that the bound static route is available.

```
<Switch-A> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6
Destination/Mask    Proto   Pre   Cost      Flags NextHop         Interface
        1.1.1.0/24  Direct  0     0           D   1.1.1.1         Vlanif10
        1.1.1.1/32  Direct  0     0           D   127.0.0.1       InLoopBack0
        1.1.1.2/32  Direct  0     0           D   1.1.1.2         Vlanif10
        2.2.2.0/24  Static  60    0           RD  1.1.1.2         Vlanif10
      127.0.0.0/8   Direct  0     0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0     0           D   127.0.0.1       InLoopBack0
```

Configuration Files

- Configuration file of Switch-A

```
#
 sysname Switch-A
#
 vlan batch 10
#
 bfd
#
interface Vlanif10
 ip address 1.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
bfd aa bind peer-ip 1.1.1.2
 discriminator local 10
 discriminator remote 20
 commit
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2 track bfd-session aa
#
return
```

- Configuration file of Switch-B

```
#
 sysname Switch-B
#
vlan batch 10 20
#
```

```
 bfd
#
interface Vlanif10
 ip address 1.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 2.2.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
bfd bb bind peer-ip 1.1.1.1
 discriminator local 20
 discriminator remote 10
 commit
#
return
```

3.2 RIP Configuration

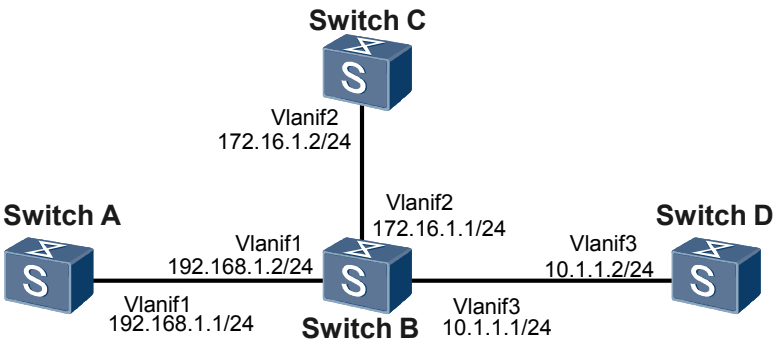
RIP can advertise and receive routes to affect the selection of data forwarding paths, and can provide the network management function. RIP is applicable to small-scale networks.

3.2.1 Example for Configuring RIP Version

Networking Requirements

As shown in **Figure 3-4**, it is required that RIP be enabled on all interfaces of SwitchA, SwitchB, SwitchC, and SwitchD and the Switchs interconnect with each other through RIP-2.

Figure 3-4 Networking diagram for configuring the RIP version number



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP address of each VLANIF interface to make the network layers accessible.

2. Enable RIP on each Switch and configure basic RIP functions.
3. Configure RIP-2 on each Switch and check the subnet masks.

Data Preparation

To complete the configuration, you need the following data:

- RIP network segment 192.168.1.0 on SwitchA
- RIP network segment 192.168.1.0, 172.16.0.0, and 10.0.0.0 on SwitchB
- RIP network segment 172.16.0.0 on SwitchC
- RIP network segment 10.0.0.0 on SwitchD
- RIP-2 on SwitchA, SwitchB, SwitchC, and SwitchD

Configuration Procedure

1. Configure the IP address of each interface

   The details are not mentioned here.

2. Configure the basic RIP functions.

   # Configure SwitchA.

```
[SwitchA] rip
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] quit
```

   # Configure SwitchB.

```
[SwitchB] rip
[SwitchB-rip-1] network 192.168.1.0
[SwitchB-rip-1] network 172.16.0.0
[SwitchB-rip-1] network 10.0.0.0
[SwitchB-rip-1] quit
```

   # Configure SwitchC.

```
[SwitchC] rip
[SwitchC-rip-1] network 172.16.0.0
[SwitchC-rip-1] quit
```

   # Configure SwitchD.

```
[SwitchD] rip
[SwitchD-rip-1] network 10.0.0.0
[SwitchD-rip-1] quit
```

   # Check the RIP routing table of SwitchA.

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------------
 Peer 192.168.1.2  on Vlanif1
      Destination/Mask        Nexthop     Cost   Tag     Flags   Sec
         10.0.0.0/8        192.168.1.2      1    0        RA      14
         172.16.0.0/16     192.168.1.2      1    0        RA      14
         192.168.1.0/24       192.168.1.2      1    0        RA      14
```

   From the routing table, you can view that the routes advertised by RIP-1 use natural masks.

3. Configure the RIP version number.

   # Configure RIP-2 on SwitchA.

```
[SwitchA] rip
[SwitchA-rip-1] version 2
[SwitchA-rip-1] quit
```

   # Configure RIP-2 on SwitchB.

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] quit
```

Configure RIP-2 on SwitchC.

```
[SwitchC] rip
[SwitchC-rip-1] version 2
[SwitchC-rip-1] quit
```

Configure RIP-2 on SwitchD.

```
[SwitchD] rip
[SwitchD-rip-1] version 2
[SwitchD-rip-1] quit
```

4. Verify the configuration.

   # Check the RIP routing table of SwitchA.

```
[SwitchA] display rip 1 route
Route Flags: R - RIP
             A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------------
 Peer 192.168.1.2  on Vlanif1
      Destination/Mask        Nexthop     Cost   Tag     Flags   Sec
         10.1.1.0/24         192.168.1.2      1    0        RA      32
         172.16.1.0/24       192.168.1.2      1    0        RA      32
         192.168.1.0/24       192.168.1.2      1    0        RA      14
```

   From the routing table, you can view that the routes advertised by RIP-2 contain accurate subnet masks.

NOTE

The aging time of a RIP route is long. Therefore, a RIP-1 route may still exist in the routing table after you configure RIP-2.

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
interface Vlanif1
ip address 192.168.1.1 255.255.255.0
#
rip 1
 version 2
 network 192.168.1.0
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
interface Vlanif1
ip address 192.168.1.2 255.255.255.0
#
interface Vlanif2
undo shutdown
 ip address 172.16.1.1 255.255.255.0
#
interface Vlanif3
 ip address 10.1.1.1 255.255.255.0
#
rip 1
 version 2
 network 192.168.1.0
 network 172.16.0.0
```

```
 network 10.0.0.0
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
interface Vlanif2
 ip address 172.16.1.2 255.255.255.0
#
rip 1
 version 2
 network 172.16.0.0
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
interface Vlanif3
 ip address 10.1.1.2 255.255.255.0
#
rip 1
 version 2
 network 10.0.0.0
#
return
```

3.2.2 Example for Configuring RIP to Import External Routes

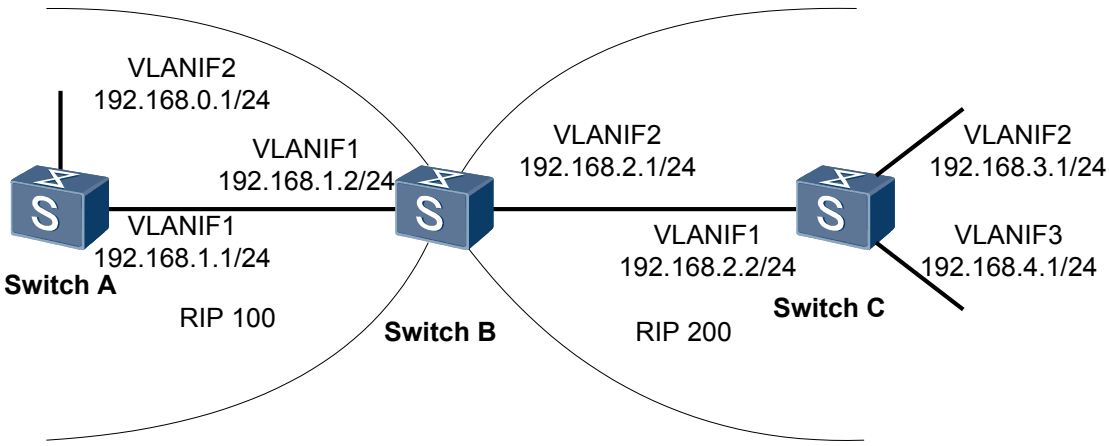
Networking Requirements

As shown in **Figure 3-5**, two RIP processes, RIP 100 and RIP 200, run on SwitchB. SwitchB exchanges routing information with SwitchA through RIP 100. SwitchB exchanges routing information with SwitchC through RIP 200.

It is required that the two processes of SwitchB import the RIP routes from each other. The cost of the imported RIP 200 routes defaults to 3.

It is required that a filtering policy be configured on SwitchB to filter out the imported RIP 200 route 192.168.4.0/24 and prevent it from being advertised to SwitchA.

Figure 3-5 Networking diagram for configuring RIP to import external routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable RIP 100 and RIP 200 on the switches according to the data shown in the preceding diagram and specify the network segments.
2. Configure the two processes on SwitchB to import the routes from each other and set the default cost of the imported RIP 200 routes to 3.
3. Configure an ACL on SwitchB to filter the routes imported from RIP 200.

Data Preparation

To complete the configuration, you need the following data:

- RIP 100 on SwitchA and the network segment 192.168.1.0 and 192.168.0.0
- RIP 100 and RIP 200 on SwitchB and the network segment 192.168.1.0 and 192.168.2.0
- RIP 200 on SwitchC and the network segment 192.168.2.0, 192.168.3.0, and 192.168.4.0
- Default cost of the imported RIP 200 routes as 3; ACL 2000 to deny the route with the source network segment of 192.168.4.0 and import RIP100 routes to RIP 200

Configuration Procedure

1. Configure the IP address of each interface.

   The details are not mentioned here.

2. Configure the basic RIP functions.

   # Enable RIP process 100 on SwitchA.

```
[SwitchA] rip 100
[SwitchA-rip-100] network 192.168.0.0
[SwitchA-rip-100] network 192.168.1.0
[SwitchA-rip-100] quit
```

   # Enable the two RIP processes, process 100 and process 200, on SwitchB.

```
[SwitchB] rip 100
[SwitchB-rip-100] network 192.168.1.0
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 192.168.2.0
[SwitchB-rip-200] quit
```

   # Enable RIP process 200 on SwitchC.

```
[SwitchC] rip 200
[SwitchC-rip-200] network 192.168.2.0
[SwitchC-rip-200] network 192.168.3.0
[SwitchC-rip-200] network 192.168.4.0
[SwitchC-rip-200] quit
```

   # Check the routing table of SwitchA.

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
      127.0.0.0/8   Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D   127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct 0    0           D   192.168.0.1     vlanif2
```

```
    192.168.0.1/32  Direct 0    0       D          127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0       D          192.168.1.1     vlanif1
    192.168.1.1/32  Direct 0    0       D          127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0       D          192.168.1.2     vlanif1
```

3. Configure RIP to import external routes.

   # Set the default route cost to 3 on SwitchB and import the routes of the two RIP processes into the routing table of each other.

```
[SwitchB] rip 100
[SwitchB-rip-100] default-cost 3
[SwitchB-rip-100] import-route rip 200
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] quit
[SwitchB-rip-200] quit
```

   # Check the routing table of SwitchA after the routes are imported.

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto  Pre  Cost   Flags    NextHop         Interface
      127.0.0.0/8   Direct 0    0        D         127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0        D         127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct 0    0       D          192.168.0.1     vlanif2
    192.168.0.1/32  Direct 0    0       D          127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0       D          192.168.1.1     vlanif1
    192.168.1.1/32  Direct 0    0       D          127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0       D          192.168.1.2     vlanif1
    192.168.2.0/24  RIP    100  4       D          192.168.1.2     vlanif1
    192.168.3.0/24  RIP    100  4       D          192.168.1.2     vlanif1
    192.168.4.0/24  RIP    100  4       D          192.168.1.2     vlanif1
```

4. Configure RIP to filter the imported routes.

   # Configure an ACL on SwitchB and set a rule to deny the packets with the source address of 192.168.4.0/24.

```
[SwitchB] acl 2000
[SwitchB-acl-basic-2000] rule deny source 192.168.4.0 0.0.0.255
[SwitchB-acl-basic-2000] rule permit
[SwitchB-acl-basic-2000] quit
```

   # Filter out the imported route 192.168.4.0/24 of RIP 200 on SwitchB according to the ACL rule.

```
[SwitchB] rip 100
[SwitchB-rip-100] filter-policy 2000 export
[SwitchB-rip-100] quit
```

5. Verify the configuration.

   # Check the routing table of SwitchA after the filtering.

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9
Destination/Mask    Proto  Pre  Cost   Flags    NextHop         Interface
      127.0.0.0/8   Direct 0    0        D         127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0        D         127.0.0.1       InLoopBack0
    192.168.0.0/24  Direct 0    0       D          192.168.0.1     vlanif2
    192.168.0.1/32  Direct 0    0       D          127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0       D          192.168.1.1     vlanif1
    192.168.1.1/32  Direct 0    0       D          127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0       D          192.168.1.2     vlanif1
    192.168.2.0/24  RIP    100  4       D          192.168.1.2     vlanif1
    192.168.3.0/24  RIP    100  4       D          192.168.1.2     vlanif1
```

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
interface vlanif2
 ip address 192.168.0.1 255.255.255.0
#
interface vlanif1
ip address 192.168.1.1 255.255.255.0
#
rip 100
 network 192.168.0.0
 network 192.168.1.0
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
acl number 2000
 rule 5 deny source 192.168.4.0 0.0.0.255
 rule 10 permit
#
interface vlanif1
ip address 192.168.1.2 255.255.255.0
#
interface vlanif2
 ip address 192.168.2.1 255.255.255.0
#
rip 100
 default-cost 3
 network 192.168.1.0
 filter-policy 2000 export
 import-route rip 200
#
rip 200
 network 192.168.2.0
 import-route rip 100
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
interface vlanif2
 ip address 192.168.3.1 255.255.255.0
#
interface vlanif3
 ip address 192.168.4.1 255.255.255.0
#
interface vlanif1
ip address 192.168.2.2 255.255.255.0
#
rip 200
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
#
return
```

3.3 RIPng Configuration

RIPng is an extension of RIP for support of IPv6.

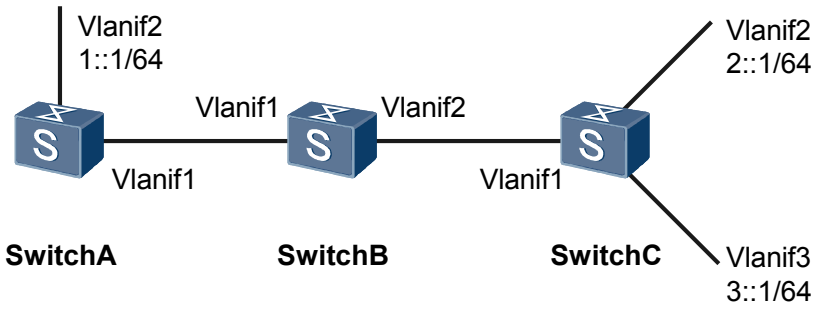
3.3.1 Example for Configuring RIPng to Filter the Received Routes

Networking Requirements

As shown in **Figure 3-6**, the prefix length of all the IPv6 addresses is 64. Besides, the adjacent Switches are connected by the IPv6 link local address.

It is required that all Switches learn IPv6 routing information in the network through RIPng; SwitchB filter out the route imported from SwitchC (3::/64), and neither add the route to the routing table of SwitchB nor advertise it to SwitchA.

Figure 3-6 Networking diagram for configuring RIPng to filter the imported routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic RIPng functions on each S-switch to connect the S-switches with each other.
2. Configure an ACL on SwitchB to filter the imported routes.

Data Preparation

To complete the configuration, you need the following data:

- Process RIPng1 enabled on each S-switch
- ACL6 2000 on SwitchB to deny the routes from the network segment 3::/64

Procedure

Step 1 Configure the IPv6 address for each interface.

The details are not mentioned here.

Step 2 Configure basic RIPng functions.

Configure SwitchA.

```
[Switch-A] ripng 1
[Switch-A-ripng-1] quit
[Switch-A] interface vlanif 2
[Switch-A-Vlanif2] ripng 1 enable
[Switch-A-Vlanif2] quit
```

```
[Switch-A] interface vlanif 1
[Switch-A-Vlanif 1] ripng 1 enable
[Switch-A-Vlanif 1] quit
```

Configure SwitchB.

```
[Switch-B] ripng 1
[Switch-B-ripng-1] quit
[Switch-B] interface vlanif 1
[Switch-B-Vlanif1] ripng 1 enable
[Switch-B-Vlanif1] quit
[Switch-B] interface vlanif 2
[Switch-B-Vlanif2] ripng 1 enable
[Switch-B-Vlanif2] quit
```

Configure SwitchC.

```
[Switch-C] ripng 1
[Switch-C-ripng-1] quit
[Switch-C] interface vlanif 1
[Switch-C-Vlanif1] ripng 1 enable
[Switch-C-Vlanif1] quit
[Switch--C] interface vlanif 2
[Switch-C-Vlanif2] ripng 1 enable
[Switch-C-Vlanif2] quit
[Switch-C] interface vlanif 3
[Switch-C-Vlanif3] ripng 1 enable
[Switch-C-Vlanif3] quit
```

Display the RIPng routing table of SwitchB.

```
[Switch-B] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------
 Peer FE80::F54C:0:9FDB:1  on Vlanif2
 Dest 2::/64,
     via FE80::F54C:0:9FDB:1, cost  1, tag 0, A, 3 Sec
 Dest 3::/64,
     via FE80::F54C:0:9FDB:1, cost  1, tag 0, A, 3 Sec
 Peer FE80::D472:0:3C23:1  on Vlanif1
 Dest 1::/64,
     via FE80::D472:0:3C23:1, cost  1, tag 0, A, 4 Sec
```

Display the RIPng routing table of SwitchA.

```
[Switch-A] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------
 Peer FE80::476:0:3624:1  on Vlanif1
 Dest 2::/64,
     via FE80::476:0:3624:1, cost  2, tag 0, A, 21 Sec
 Dest 3::/64,
     via FE80::476:0:3624:1, cost  2, tag 0, A, 21 Sec
```

Step 3 Configure SwitchB to filter the imported routes.

```
[Switch-B] acl ipv6 number 2000
[Switch-B-acl6-basic-2000] rule deny source 3:: 64
[Switch-B-acl6-basic-2000] rule permit
[Switch-B-acl6-basic-2000] quit
[Switch-B] ripng 1
[Switch-B-ripng-1] filter-policy 2000 import
[Switch-B-ripng-1] quit
```

Step 4 Verify the configuration.

Check that the RIPng routing table of Switch-B contains no route of the network segment 3::/64.

```
[Switch-B] display ripng 1 route
```

```
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------
Peer FE80::F54C:0:9FDB:1  on Vlanif2
Dest 2::/64,
    via FE80::F54C:0:9FDB:1, cost  1, tag 0, A, 14 Sec
Peer FE80::D472:0:3C23:1  on Vlanif1
Dest 1::/64,
    via FE80::D472:0:3C23:1, cost  1, tag 0, A, 25 Sec
[Switch-A] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------
Peer FE80::476:0:3624:1  on Vlanif1
Dest 2::/64,
    via FE80::476:0:3624:1, cost  2, tag 0, A, 7 Sec
```

----End

Configuration Files

- Configuration file of Switch-A

```
#
 sysname Switch-A
#
 ipv6
#
interface Vlanif1
ipv6 address auto link-local
 ripng 1 enable
#
interface Vlanif2
 ipv6 address 1::1/64
 ripng 1 enable
#
ripng 1
#
return
```

- Configuration file of Switch-B

```
#
 sysname Switch-B
#
 ipv6
#
acl ipv6 number 2000
 rule 0 deny source 3::/64
 rule 1 permit
#
interface Vlanif1
 ipv6 address auto link-local
 ripng 1 enable
#
interface Vlanif2
 ipv6 address auto link-local
 ripng 1 enable
#
ripng 1
 filter-policy 2000 import
#
return
```

- Configuration file of Switch-C

```
#
 sysname Switch-C
#
 ipv6
#
interface Vlanif1
 ipv6 address auto link-local
```

```
 ripng 1 enable
#
interface Vlanif2
 ipv6 address 2::1/64
 ripng 1 enable
#
interface Vlanif3
 ipv6 address 3::1/64
 ripng 1 enable
#
ripng 1
#
return
```

3.4 OSPF Configuration

OSPF, which is developed by the IETF, is a link-state IGP. OSPF is widely used in access networks and MANs.

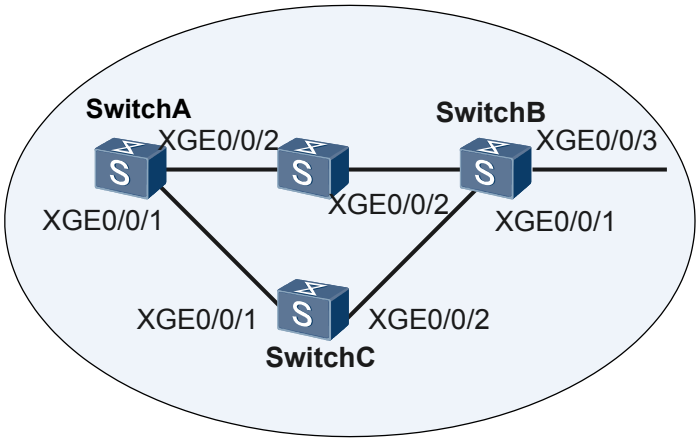
3.4.1 Example for Configuring BFD for OSPF

Networking Requirements

As shown in **Figure 3-7**, the networking requirements are as follows:

- Switch A, Switch B, and Switch C run OSPF.
- BFD for OSPF is enabled on Switch A, Switch B, and Switch C.
- Service traffic is transmitted on the main link Switch A→Switch B. Link Switch A→Switch C→Switch B is a backup link.
- BFD is configured on the interfaces between Switch A and Switch B. When a fault occurs on the link between the Switch s, BFD can quickly detect the fault and notify OSPF of the fault. Then, the service flow is transmitted on the backup link.

Figure 3-7 Networking diagram for configuring BFD for OSPF



Switch	Interface	VLANIF interface	IP address
Switch A	XGE0/0/1	VLANIF 10	1.1.1.1/24
Switch A	XGE0/0/2	VLANIF 20	3.3.3.1/24
Switch B	XGE0/0/1	VLANIF 30	2.2.2.2/24

Switch B	XGE0/0/2	VLANIF 20	3.3.3.2/24
Switch B	XGE0/0/3	VLANIF 40	172.16.1.1/24
Switch C	XGE0/0/1	VLANIF 10	1.1.1.2/24
Switch C	XGE0/0/2	VLANIF 30	2.2.2.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the basic OSPF functions on the Switch s.
2. Enable the BFD feature globally.
3. Enable BFD for OSPF on Switch A and Switch B.

Data Preparation

To complete the configuration, you need the following data:

- ID of the VLAN that each interface belongs to, as shown in **Figure 3-7**
- IP address of each VLANIF interface, as shown in **Figure 3-7**
- Router ID and OSPF process ID of each Switch and network segments that OSPF interfaces belong to:
  - On Switch A, the router ID is 1.1.1.1; OSPF process ID is 1; the network segments of Area 0 are 3.1.1.0/24 and 1.1.1.0/24.
  - On Switch B, the router ID is 2.2.2.2; OSPF process ID is 1; the network segments of Area 0 are 3.1.1.0/24, 2.2.2.0/24, and 172.16.1.0/24.
  - On Switch C, the router ID is 3.3.3.3; the OSPF process ID is 1; the network segments of Area 0 are 192.168.1.0/24 and 172.16.1.0/24.
- Minimum interval for sending the BFD packets, minimum interval for receiving the BFD packets, and local detection time multiplier on Switch A and Switch B

Procedure

Step 1 Create VLANs and add corresponding interfaces to the VLANs.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
[SwitchA] interface XGigabitEthernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface XGigabitEthernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid pvid vlan 20
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-XGigabitEthernet0/0/2] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Step 2 Assign an IP address to each VLANIF interface.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 1.1.1.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 3.3.3.1 24
[SwitchA-Vlanif20] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Step 3 Configure the basic OSPF functions. See Example for Configuring Basic OSPF Functions.

Step 4 Configure BFD for OSPF.

Enable BFD globally on Switch A.

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] ospf
[SwitchA-ospf-1] bfd all-interfaces enable
[SwitchA-ospf-1] quit
```

Enable BFD globally on Switch B.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] ospf
[SwitchB-ospf-1] bfd all-interfaces enable
[SwitchB-ospf-1] quit
```

Run the **display ospf bfd session all** command on Switch A or Switch B. You can see that the BFD state is Up.

Take Switch A for example. The display is as follows:

```
[SwitchA] display ospf bfd session all
          OSPF Process 1 with Router ID 1.1.1.1
  Area 0.0.0.0 interface  3.3.3.1(Vlanif20)'s BFD Sessions

 NeighborId:2.2.2.2          AreaId:0.0.0.0          Interface:Vlanif20
 BFDState:up                 rx    :1000             tx       :1000
 Multiplier:3                BFD Local Dis:8195      LocalIpAdd:3.3.3.1
 RemoteIpAdd:3.3.3.2         Diagnostic Info:No diagnostic information

  Area 0.0.0.0 interface 1.1.1.1(Vlanif10)'s BFD Sessions

 NeighborId:3.3.3.3          AreaId:0.0.0.0          Interface:Vlanif10
 BFDState:up                 rx    :1000             tx       :1000
 Multiplier:3                BFD Local Dis:8194      LocalIpAdd1:1.1.1.1
 RemoteIpAdd:1.1.1.2         Diagnostic Info:No diagnostic information
```

Step 5 Configure the BFD feature of interfaces.

Configure BFD on VLANIF 20 of Switch A, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiplier to 4.

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ospf bfd enable
[SwitchA-Vlanif20] ospf bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
[SwitchA-Vlanif20] quit
```

Configure BFD on VLANIF20 of Switch B and set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms and the local detection time multiplier to 4.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] ospf bfd enable
[SwitchB-Vlanif20] ospf bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
[SwitchB-Vlanif20] quit
```

Run the **display ospf bfd session all** command on Switch A or Switch B. You can see that the BFD state is Up.

Take Switch B for example. The display is as follows:

```
[SwitchB] display ospf bfd session all

         OSPF Process 1 with Router ID 2.2.2.2
 Area 0.0.0.0 interface 3.3.3.2(Vlanif20)'s BFD Sessions

 NeighborId:1.1.1.1          AreaId:0.0.0.0          Interface: Vlanif20
 BFDState:up                 rx    :100             tx       :100
 Multiplier:4                BFD Local Dis:8198      LocalIpAdd:3.3.3.2
 RemoteIpAdd:3.3.3.1         Diagnostic Info:No diagnostic information

  Area 0.0.0.0 interface 2.2.2.2(Vlanif30)'s BFD Sessions

 NeighborId:3.3.3.3          AreaId:0.0.0.0          Interface: Vlanif30
 BFDState:up                 rx    :1000              tx       :1000
 Multiplier:3                BFD Local Dis:8199      LocalIpAdd:2.2.2.2
 RemoteIpAdd:2.2.2.1         Diagnostic Info:No diagnostic information
```

Step 6 Verify the configuration.

Run the **shutdown** command on VLANIF 20 of Switch B to simulate a link fault.

```
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] shutdown
```

View the routing table of Switch A.

```
<SwitchA> display ospf routing

         OSPF Process 1 with Router ID 1.1.1.1 Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.1/24      3     Stub       1.1.1.2         2.2.2.2         0.0.0.0
 3.3.3.0/24         1     Stub       3.3.3.1         1.1.1.1         0.0.0.0
 2.2.2.0/24         2     Transit    1.1.1.2         3.3.3.3         0.0.0.0
 1.1.1.0/24         1     Transit    1.1.1.1         1.1.1.1         0.0.0.0

 Total Nets: 4 Intra Area: 4  Inter Area: 0  ASE: 0  NSSA: 0
```

As shown in the OSPF routing table, the backup link Switch A→Switch C→Switch B takes effect after the main link fails. The next hop address of the route to 172.16.1.0/24 becomes 1.1.1.2.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 router id 1.1.1.1
#
 vlan batch 10 20
```

```
#
 bfd
#
interface Vlanif10
 ip address 1.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 3.3.3.1 255.255.255.0
 ospf bfd enable
 ospf bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ospf 1
 bfd all-interface enable
 area 0.0.0.0
  network 3.3.3.0 0.0.0.255
  network 1.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 router id 2.2.2.2
#
vlan batch 20 30 40
#
 bfd
#
interface Vlanif20
 ip address 3.3.3.2 255.255.255.0
 ospf bfd enable
 ospf bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
#
interface Vlanif30
 ip address 2.2.2.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 20
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
ospf 1
 bfd all-interface enable
 area 0.0.0.0
  network 3.3.3.0 0.0.0.255
  network 2.2.2.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 router id 3.3.3.3
#
 vlan batch 10 30
#
 bfd
#
interface Vlanif10
 ip address 1.1.1.2 255.255.255.0
#
interface Vlanif30
 ip address 2.2.2.1 255.255.255.0
 ospf bfd enable
 ospf bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 bfd all-interface enable
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 2.2.2.0 0.0.0.255
#
return
```

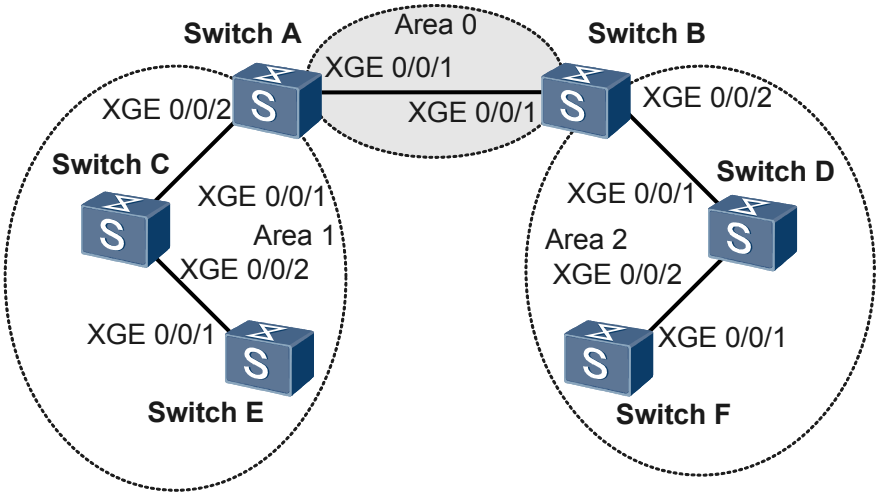
3.4.2 Example for Configuring Basic OSPF Functions

Networking Requirements

As shown in **Figure 3-8**, all switches run OSPF, and the entire AS is partitioned into three areas. Switch A and Switch B serve as ABRs to forward routes between areas.

After the configuration, each Switch should learn the routes to all network segments from the AS.

Figure 3-8 Networking diagram of basic OSPF configurations



Switch	Interface	VLANIF Interface	IP Address
Switch A	XGE0/0/1	VLANIF 10	192.168.0.1/24
Switch A	XGE 0/0/2	VLANIF 20	192.168.1.1/24
Switch B	XGE 0/0/1	VLANIF 10	192.168.0.2/24
Switch B	XGE 0/0/2	VLANIF 30	192.168.2.1/24
Switch C	XGE 0/0/1	VLANIF 20	192.168.1.2/24
Switch C	XGE 0/0/2	VLANIF 40	172.16.1.1/24
Switch D	XGE 0/0/1	VLANIF 30	192.168.2.2/24
Switch D	XGE 0/0/2	VLANIF 50	172.17.1.1/24
Switch E	XGE 0/0/1	VLANIF 40	172.16.1.2/24
Switch F	XGE 0/0/1	VLANIF 50	172.17.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of a VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Enable OSPF on each Switch and specify network segments in different areas.
4. Check the routing table and LSDB.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN that each interface belongs to is shown in **Figure 3-8**.
- The IP address of each interface is shown in **Figure 3-8**.
- The router ID of each Switch, the OSPF process ID, and the area to which each interface belongs are as follows.

- The router ID of Switch A is 1.1.1.1, the OSPF process ID is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 1 is 192.168.1.0/24.
- The router ID of Switch B is 2.2.2.2, the OSPF process ID is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 2 is 192.168.2.0/24.
- The router ID of Switch C is 3.3.3.3, the OSPF process ID is 1, the network segments of Area 1 are 192.168.1.0/24 and 172.16.1.0/24.
- The router ID of Switch D is 4.4.4.4, the OSPF process ID is 1, and the network segments of Area 2 are 192.168.2.0/24 and 172.17.1.0/24.
- The router ID of Switch E is 5.5.5.5, the OSPF process ID is 1, and the network segment of Area 1 is 172.16.1.0/24.
- The router ID of Switch F is 6.6.6.6, the OSPF process ID is 1, and the network segment of Area 2 is 172.17.1.0/24.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.

2. Assign an IP address to each interface.

   The configuration details are not mentioned here.

3. Configuring Basic OSPF Functions.

   # Configure Switch A.

```
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

   # Configure Switch B.

```
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

   # Configure Switch C.

```
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

   # Configure Switch D.

```
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
```

```
[SwitchD-ospf-1] quit
```

Configure Switch E.

```
[SwitchE] router id 5.5.5.5
[SwitchE] ospf
[SwitchE-ospf-1] area 1
[SwitchE-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.1] quit
[SwitchE-ospf-1] quit
```

Configure Switch F.

```
[SwitchF] router id 6.6.6.6
[SwitchF] ospf
[SwitchF-ospf-1] area 2
[SwitchF-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchF-ospf-1-area-0.0.0.2] quit
[SwitchF-ospf-1] quit
```

4. Verify the configuration.

Check OSPF neighbors of Switch A.

```
[SwitchA] display ospf peer
          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 192.168.0.1(Vlanif10)'s neighbors
 Router ID: 2.2.2.2      Address: 192.168.0.2      GR State: Normal
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.0.1  BDR: 192.168.0.2  MTU: 0
   Dead timer due in 36  sec
   Neighbor is up for 00:15:04
   Authentication Sequence: [ 0 ]

                  Neighbors

 Area 0.0.0.1 interface 192.168.1.1(Vlanif20)'s neighbors
 Router ID: 3.3.3.3       Address: 192.168.1.2      GR State: Normal
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 192.168.1.1  BDR: 192.168.1.2  MTU: 0
   Dead timer due in 39  sec
   Neighbor is up for 00:07:32
   Authentication Sequence: [ 0 ]
```

Check OSPF routing information of Switch A.

```
[SwitchA] display ospf routing

          OSPF Process 1 with Router ID 1.1.1.1
                   Routing Tables

 Routing for Network
 Destination      Cost  Type         NextHop         AdvRouter       Area
 172.16.1.0/24     2    Transit      192.168.1.2     3.3.3.3         0.0.0.1
 172.17.1.0/24     3    Inter-area   192.168.0.2     2.2.2.2         0.0.0.0
 192.168.0.0/24    1    Transit      192.168.0.1     1.1.1.1         0.0.0.0
 192.168.1.0/24    1    Transit      192.168.1.1     1.1.1.1         0.0.0.1
 192.168.2.0/24    2    Inter-area   192.168.0.2     2.2.2.2         0.0.0.0

 Total Nets: 5
 Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

View the LSDB of Switch A.

```
[SwitchA] display ospf lsdb

          OSPF Process 1 with Router ID 1.1.1.1
                  Link State Database

                        Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    2.2.2.2          2.2.2.2            317  48    80000003    1
 Router    1.1.1.1          1.1.1.1            316  48    80000002    1
```

```
 Network   192.168.0.1     1.1.1.1           316  32    80000001    0
 Sum-Net   172.16.1.0      1.1.1.1           250  28    80000001    2
 Sum-Net   172.17.1.0      2.2.2.2           203  28    80000001    2
 Sum-Net   192.168.2.0     2.2.2.2           237  28    80000002    1
 Sum-Net   192.168.1.0     1.1.1.1           295  28    80000002    1

                        Area: 0.0.0.1
Type      LinkState ID    AdvRouter         Age  Len   Sequence   Metric
 Router    192.168.1.2     192.168.1.2       188  48    80000002    1
 Router    5.5.5.5          5.5.5.5           214  36    80000004    1
 Router    3.3.3.3          3.3.3.3           217  60    80000008    1
 Router    1.1.1.1          1.1.1.1           289  48    80000002    1
 Sum-Net   172.17.1.0      1.1.1.1           202  28    80000002    3
 Network   172.16.1.1      3.3.3.3           670  32    80000001    0
 Sum-Net   172.17.1.0      1.1.1.1           202  28    80000001    3
 Sum-Net   192.168.2.0     1.1.1.1           242  28    80000001    2
 Sum-Net   192.168.0.0     1.1.1.1           300  28    80000001    1
```

Check the routing table of Switch D and perform the ping operation to test the connectivity.

```
[SwitchD] display ospf routing

          OSPF Process 1 with Router ID 4.4.4.4
                  Routing Tables

 Routing for Network
 Destination        Cost  Type         NextHop         AdvRouter       Area
 172.16.1.0/24      4     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 172.17.1.0/24      1     Transit     172.17.1.1      4.4.4.4         0.0.0.2
 192.168.0.0/24     2     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 192.168.1.0/24     3     Inter-area 192.168.2.1     2.2.2.2         0.0.0.2
 192.168.2.0/24     1     Transit     192.168.2.2     4.4.4.4         0.0.0.2

 Total Nets: 5
 Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0

[SwitchD] ping 172.16.1.1
  PING 172.16.1.1: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=253 time=62 ms
    Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=253 time=16 ms
    Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=253 time=62 ms
    Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=253 time=94 ms
    Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=253 time=63 ms

  --- 172.16.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 16/59/94 ms
```

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
```

```
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
 ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
router id 2.2.2.2
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 192.168.0.2 255.255.255.0
#
interface Vlanif30
 ip address 192.168.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
router id 4.4.4.4
```

```
#
 vlan batch 30 50
#
interface Vlanif30
 ip address 192.168.2.2 255.255.255.0
#
interface Vlanif50
 ip address 172.17.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 50
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
```

- Configuration file of Switch E

```
#
 sysname SwitchE
#
router id 5.5.5.5
#
 vlan batch 40
#
interface Vlanif40
 ip address 172.16.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Switch F

```
#
 sysname SwitchF
#
router id 6.6.6.6
#
 vlan batch 50
#
interface Vlanif50
 ip address 172.17.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 50
#
ospf 1
 area 0.0.0.2
  network 172.17.1.0 0.0.0.255
#
return
```

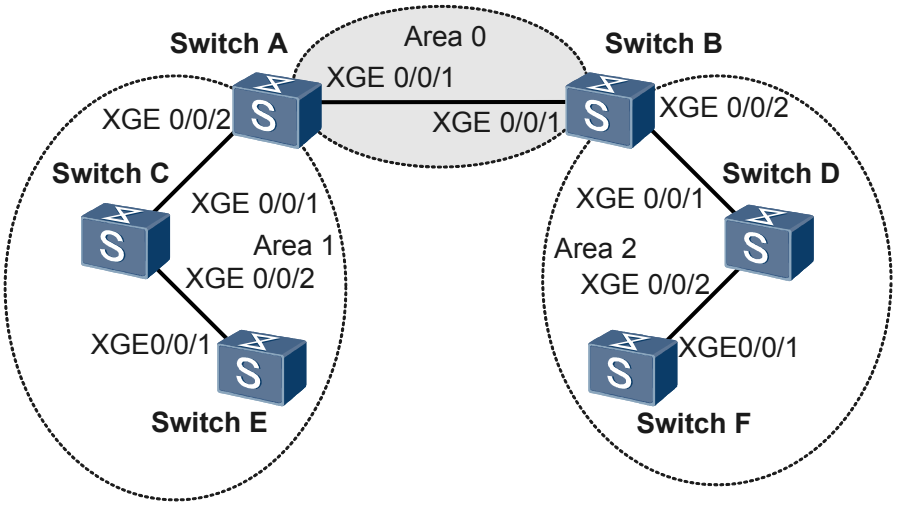
3.4.3 Example for Configuring a Stub Area of OSPF

Networking Requirements

As shown in **Figure 3-9**, OSPF is enabled on all Switchs and the entire AS is partitioned into three areas. SwitchA and SwitchB function as ABRs to forward routes between areas. SwitchD functions as the ASBR to import static routes.

The requirement is to configure Area 1 as the stub area, thus reducing the LSAs advertised to this area without affecting the route reachability.

Figure 3-9 Configuring OSPF stub areas



S-switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	192.168.0.1/24
SwitchA	XGE 0/0/2	VLANIF 20	192.168.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	192.168.0.2/24
SwitchB	XGE 0/0/2	VLANIF 30	192.168.2.1/24
SwitchC	XGE 0/0/1	VLANIF 20	192.168.1.2/24
SwitchC	XGE 0/0/2	VLANIF 40	172.16.1.1/24
SwitchD	XGE 0/0/1	VLANIF 30	192.168.2.2/24
SwitchD	XGE 0/0/2	VLANIF 50	172.17.1.1/24
SwitchE	XGE 0/0/1	VLANIF 40	172.16.1.2/24
SwitchF	XGE 0/0/1	VLANIF 50	172.17.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each Switch and configure basic OSPF functions.
2. Configure static routes on SwitchD and import them.

3. Configure Area 1 as a stub area. You need to run the **stub** command on all Switchs in Area 1.
4. Do not advertise Type3 LSAs to the stub area on SwitchA.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in **Figure 3-9**.
- The IP address of each interface is shown in **Figure 3-9**.
- The router ID of each Switch, the OSPF process ID, and the area to which each interface belongs are as follows:
  - The router ID of SwitchA is 1.1.1.1, the OSPF process ID is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 1 is 192.168.1.0/24.
  - The router ID of SwitchB is 2.2.2.2, the OSPF process ID is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 2 is 192.168.2.0/24.
  - The router ID of SwitchC is 3.3.3.3, the OSPF process ID is 1, and the network segments of Area 1 are 192.168.1.0/24 and 172.16.1.0/24.
  - The router ID of SwitchD is 4.4.4.4, the OSPF process ID is 1, and the network segments of Area 2 are 192.168.2.0/24 and 172.17.1.0/24.
  - The router ID of SwitchE is 5.5.5.5, the OSPF process ID is 1, and the network segment of Area 1 is 172.16.1.0/24.
  - The router ID of SwitchF is 6.6.6.6, the OSPF process ID is 1, and the network segment of Area 2 is 172.17.1.0/24.

Configuration Procedure

1. **3.4.2 Example for Configuring Basic OSPF Functions**.
2. Configure SwitchD to import static routes.

   # Import static routes on SwitchD, as follows:

```
[SwitchD] ip route-static 200.0.0.0 8 null 0
[SwitchD] ospf
[SwitchD-ospf-1] import-route static type 1
[SwitchD-ospf-1] quit
```

   # Display the ABR or ASBR of SwitchC.

```
[SwitchC] display ospf abr-asbr

          OSPF Process 1 with Router ID 3.3.3.3
                  Routing Table to ABR and ASBR

 Type        Destination       Area       Cost  Nexthop         RtType
 Intra-area  1.1.1.1           0.0.0.1    1     192.168.1.1     ABR
 Inter-area  4.4.4.4           0.0.0.1    3     192.168.1.1     ASBR
```

   # Check the routing table of an OSPF process of SwitchC.

```
[SwitchC] display ospf routing

     OSPF Process 1 with Router ID 3.3.3.3
                 Routing Tables

 Routing for Network
 Destination        Cost  Type        NextHop         AdvRouter       Area
 172.16.1.0/24      1     Transit     172.16.1.1      3.3.3.3         0.0.0.1
 172.17.1.0/24      4     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 192.168.0.0/24     2     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
```

```
192.168.1.0/24     1     Transit     192.168.1.2     3.3.3.3         0.0.0.1
192.168.2.0/24     3     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1

Routing for ASEs
Destination        Cost      Type       Tag         NextHop         AdvRouter
200.0.0.0/8        4      Type1      1           192.168.1.1     4.4.4.4

Total Nets: 6
Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

If the area where SwitchC resides is the common area, you can view that AS external routes exist in the routing table.

3. Configure Area 1 as a stub area.

   # Configure SwitchA.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

   # Configure SwitchC.

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

   # Configure SwitchE.

```
[SwitchE] ospf
[SwitchE-ospf-1] area 1
[SwitchE-ospf-1-area-0.0.0.1] stub
[SwitchE-ospf-1-area-0.0.0.1] quit
[SwitchE-ospf-1] quit
```

   # Check the routing table of SwitchC.

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 3.3.3.3
                  Routing Tables

 Routing for Network
 Destination        Cost  Type        NextHop         AdvRouter       Area
 0.0.0.0/0           2    Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 172.16.1.0/24       1    Transit     172.16.1.1      3.3.3.3         0.0.0.1
 172.17.1.0/24       4    Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 192.168.0.0/24      2    Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 192.168.1.0/24      1    Transit     192.168.1.2     3.3.3.3         0.0.0.1
 192.168.2.0/24      3    Inter-area  192.168.1.1     1.1.1.1         0.0.0.1

 Total Nets: 6
 Intra Area: 2  Inter Area: 4  ASE: 0  NSSA: 0
```

   When the area where SwitchC resides is configured as a stub area, you may not find the AS external route but a default route external to the AS.

   # Disable Router A from advertising Type3 LSAs to the stub area.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

4. Verify the configuration.

   # Check the OSPF routing table of SwitchC.

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 3.3.3.3
```

```
                  Routing Tables

 Routing for Network
 Destination        Cost  Type           NextHop         AdvRouter       Area
 0.0.0.0/0           2    Inter-area     192.168.1.1     1.1.1.1         0.0.0.1
 172.16.1.0/24       1    Transit        172.16.1.1      3.3.3.3         0.0.0.1
 192.168.1.0/24      1    Transit        192.168.1.2     3.3.3.3         0.0.0.1

 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

After the advertisement of Summary-LSA to the stub area is disabled, the route entries are further reduced. The AS external routes are invisible in the routing table. Instead, there is a default route.

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  stub no-summary
#
return
```

NOTE

Configuration files of SwitchB and SwitchF are the same as the configuration file of SwitchA, and are not mentioned here.

- Configuration file of SwitchC

```
#
 sysname SwitchC
# router id 3.3.3.3
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 40
```

```
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
  stub
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 vlan batch 30 50
#
router id 4.4.4.4
#
interface Vlanif30
 ip address 192.168.2.2 255.255.255.0
#
interface Vlanif50
 ip address 172.17.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 50
#
ospf 1
 import-route static type 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
 ip route-static 200.0.0.0 255.0.0.0 NULL0
#
return
```

- Configuration file of SwitchE

```
#
 sysname SwitchE
#
router id 5.5.5.5
#
 vlan batch 40
#
interface Vlanif40
 ip address 172.16.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
  stub
#
return
```

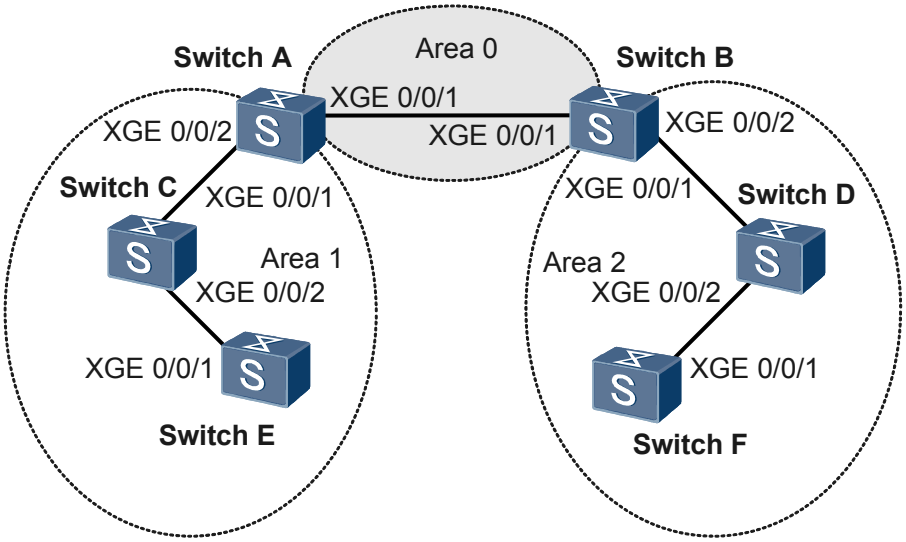
3.4.4 Example for Configuring an OSPF NSSA Area

Networking Requirements

As shown in **Figure 3-10**, OSPF is enabled on all Switches and the entire AS is partitioned into three areas. SwitchA and SwitchB function as ABRs to forward routes between areas. SwitchD functions as the ASBR to import external routes (static routes).

The requirement is to configure Area 1 as an NSSA area and configure SwitchC as an ASBR to import external routes (static routes). The routing information can be transmitted correctly in the AS.

Figure 3-10 Configuring OSPF NSSA areas



S-switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	192.168.0.1/24
SwitchA	XGE 0/0/2	VLANIF 20	192.168.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	192.168.0.2/24
SwitchB	XGE 0/0/2	VLANIF 30	192.168.2.1/24
SwitchC	XGE 0/0/1	VLANIF 20	192.168.1.2/24
SwitchC	XGE 0/0/2	VLANIF 40	172.16.1.1/24
SwitchD	XGE 0/0/1	VLANIF 30	192.168.2.2/24
SwitchD	XGE 0/0/2	VLANIF 50	172.17.1.1/24
SwitchE	XGE 0/0/1	VLANIF 40	172.16.1.2/24
SwitchF	XGE 0/0/1	VLANIF 50	172.17.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each Switch and configure basic OSPF functions.
2. Configure static routes on SwitchD and import them into OSPF.
3. Configure Area 1 as an NSSA area (run the **nssa** command on all routers in Area 1) and check the OSPF routing information of SwitchC.
4. Configure static routes on SwitchC, import them into OSPF, and check the OSPF routing information of SwitchD.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in **Figure 3-10**.
- The IP address of each interface is shown in **Figure 3-10**.
- The router ID of each Switch, the OSPF process ID, and the area to which each interface belongs are as follows:
  - The router ID of SwitchA is 1.1.1.1, the OSPF process ID is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 1 is 192.168.1.0/24.
  - The router ID of SwitchB is 2.2.2.2, the OSPF process ID is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 2 is 192.168.2.0/24.
  - The router ID of SwitchC is 3.3.3.3, the OSPF process ID is 1, and the network segments of Area 1 are 192.168.1.0/24 and 172.16.1.0/24.
  - The router ID of SwitchD is 4.4.4.4, the OSPF process ID is 1, and the network segments of Area 2 are 192.168.2.0/24 and 172.16.1.0/24.
  - The router ID of SwitchE is 5.5.5.5, the OSPF process ID is 1, and the network segment of Area 1 is 172.16.1.0/24.
  - The router ID of SwitchF is 6.6.6.6, the OSPF process ID is 1, and the network segment of Area 2 is 172.17.1.0/24.

Configuration Procedure

1. **3.4.2 Example for Configuring Basic OSPF Functions**.
2. Configure SwitchD to import static routes. See **3.4.3 Example for Configuring a Stub Area of OSPF**.
3. Configure Area 1 as an NSSA area.

   # Configure SwitchA.

   ```
   [SwitchA] ospf
   [SwitchA-ospf-1] area 1
   [SwitchA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary
   [SwitchA-ospf-1-area-0.0.0.1] quit
   [SwitchA-ospf-1] quit
   ```

   # Configure SwitchC.

   ```
   [SwitchC] ospf
   [SwitchC-ospf-1] area 1
   [SwitchC-ospf-1-area-0.0.0.1] nssa
   [SwitchC-ospf-1-area-0.0.0.1] quit
   [SwitchC-ospf-1] quit
   ```

   # Configure SwitchE.

   ```
   [SwitchE] ospf
   [SwitchE-ospf-1] area 1
   [SwitchE-ospf-1-area-0.0.0.1] nssa
   [SwitchE-ospf-1-area-0.0.0.1] quit
   [SwitchE-ospf-1] quit
   ```

   NOTE

   You should run the **default-route-advertise no-summary** command on SwitchA. In this manner, the size of the routing table of devices in the NSSA area can be reduced. For other devices in the NSSA area, you need to use only the **nssa** command.

   # Check the OSPF routing table of SwitchC.

   ```
   [SwitchC] display ospf routing
   ```

```
          OSPF Process 1 with Router ID 3.3.3.3
                  Routing Tables

 Routing for Network
 Destination        Cost  Type          NextHop         AdvRouter       Area
 0.0.0.0/0           2     Inter-area  192.168.1.1     1.1.1.1         0.0.0.1
 172.16.1.0/24      1     Transit      172.16.1.1      3.3.3.3         0.0.0.1
 192.168.1.0/24     1     Transit      192.168.1.2     3.3.3.3         0.0.0.1

 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

4. Configure SwitchC to import static routes.

   # Import static routes on SwitchC, as follows:

```
[SwitchC]ip route-static 100.0.0.0 8 null 0
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

5. Verify the configuration.

   # Check the OSPF routing table of SwitchD.

```
[SwitchD] display ospf routing

          OSPF Process 1 with Router ID 4.4.4.4
                  Routing Tables

 Routing for Network
 Destination        Cost  Type         NextHop         AdvRouter       Area
 172.16.1.0/24      4     Inter-area   192.168.2.1     2.2.2.2         0.0.0.2
 172.17.1.0/24      1     Transit      172.17.1.1      4.4.4.4         0.0.0.2
 192.168.0.0/24     2     Inter-area   192.168.2.1     2.2.2.2         0.0.0.2
 192.168.1.0/24     3     Inter-area   192.168.2.1     2.2.2.2         0.0.0.2
 192.168.2.0/24     1     Transit      192.168.2.2     4.4.4.4         0.0.0.2
 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop         AdvRouter
 100.0.0.0/8        1         Type2      1           192.168.2.1     1.1.1.1

 Total Nets: 6
 Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

   You can view one imported AS external route on SwitchD in the NSSA area.

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
```

```
  network 192.168.1.0 0.0.0.255
  nssa default-route-advertise no-summary
#
return
```

NOTE

Configuration files of SwitchB, SwitchD, and SwitchF are the same as the configuration file of SwitchA, and are not mentioned here.

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1
 import-route static
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
  nssa
#
 ip route-static 100.0.0.0 255.0.0.0 NULL0
#
return
```

- Configuration file of SwitchE

```
#
 sysname SwitchE
#
router id 5.5.5.5
#
 vlan batch 40
#
interface Vlanif40
 ip address 172.16.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
  nssa
#
return
```

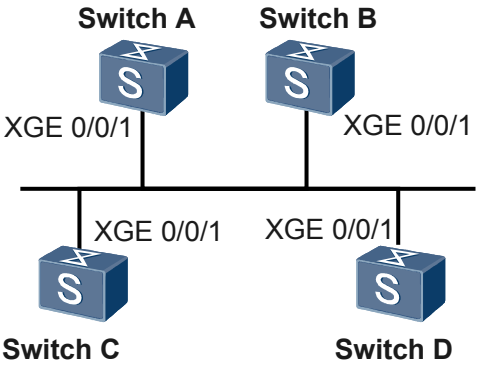
3.4.5 Example for Configuring DR Election of an OSPF Process

Networking Requirements

As shown in **Figure 3-11**, Switch A has the highest priority of 100 in the network and is selected as DR. Switch C has the second highest priority, and is selected as BDR. The priority of Switch

B is 0, so Switch B cannot be selected as DR. The priority of Switch D is not configured and its default value is 1.

Figure 3-11 Networking diagram for configuring DR election of an OSPF process



Switch	Interface	VLANIF	IP address
SwitchA	XGE 0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	192.168.1.2/24
SwitchC	XGE 0/0/1	VLANIF 10	192.168.1.3/24
SwitchD	XGE 0/0/1	VLANIF 10	192.168.1.4/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of a VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure the router ID of each Switch, enable OSPF, and specify network segments.
4. Check the DR or BDR status of each Switch.
5. Set the DR priority of the interface and check the DR or BDR status.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in **Figure 3-11**.
- The IP address of each interface is shown in **Figure 3-11**.
- The router ID of each Switch, the OSPF process ID, the area to which each interface belongs, and DR priority are as follows:
  - The router ID of Switch A is 1.1.1.1, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 100.
  - The router ID of Switch B is 2.2.2.2, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 0.

- The router ID of Switch C is 3.3.3.3, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 2.
- The router ID of Switch B is 4.4.4.4, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 1.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.

2. Assign an IP address to each interface.

   The configuration details are not mentioned here.

3. **3.4.2 Example for Configuring Basic OSPF Functions**.

   # Configure Switch A.

```
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # Configure Switch B.

```
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

   # Configure Switch C.

```
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

   # Configure Switch D.

```
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

   # Check the DR or BDR status.

```
[SwitchA] display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
                 Neighbors

Area 0.0.0.0 interface 192.168.1.1(Vlanif10)'s neighbors
Router ID: 2.2.2.2      Address: 192.168.1.2
  State: 2-Way  Mode:Nbr is  Master  Priority: 1
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 32  sec
  Retrans timer interval: 5
  Neighbor is up for 00:00:00
  Authentication Sequence: [ 0 ]

Router ID: 3.3.3.3      Address: 192.168.1.3
  State: Full  Mode:Nbr is  Master  Priority: 1
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
```

```
  Dead timer due in 37  sec
  Retrans timer interval: 5
  Neighbor is up for 00:04:06
  Authentication Sequence: [ 0 ]

 Router ID: 4.4.4.4      Address: 192.168.1.4
  State: Full  Mode:Nbr is  Master  Priority: 1
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 37  sec
  Retrans timer interval: 5
  Neighbor is up for 00:03:53
  Authentication Sequence: [ 0 ]
```

Check information about the neighbor of Switch A. You can view the DR priority and neighbor status. By default, the DR priority is 1. Now Switch D is a DR and Switch C is a BDR.

NOTE

When the priority is the same, the Switch with a higher router ID is selected as DR. If one Ethernet interface of the Switch becomes DR, the other broadcast interfaces of the Switch have a high priority of being selected as DRs in future DR selection. That is, select the DR Switch as DR. DR cannot be preempted.

4. Configure DR priorities on the interfaces.

   # Configure Switch A.

```
[SwitchA] interface Vlanif 10
[SwitchA-Vlanif10] ospf dr-priority 100
[SwitchA-Vlanif10] quit
```

   # Configure Switch B.

```
[SwitchB] interface Vlanif 10
[SwitchB-Vlanif10] ospf dr-priority 0
[SwitchB-Vlanif10] quit
```

   # Configure Switch C.

```
[SwitchC] interface Vlanif 10
[SwitchC-Vlanif10] ospf dr-priority 2
[SwitchC-Vlanif10] quit
```

   # View the DR or BDR status.

```
 [SwitchD] display ospf peer

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlanif10)'s neighbors
 Router ID: 1.1.1.1      Address: 192.168.1.1
   State: Full  Mode:Nbr is  Slave  Priority: 100
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 31  sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:17
   Authentication Sequence: [ 0 ]
 Router ID: 2.2.2.2      Address: 192.168.1.2
   State: Full  Mode:Nbr is  Slave  Priority: 0
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:19
   Authentication Sequence: [ 0 ]

 Router ID: 3.3.3.3      Address: 192.168.1.3
   State: Full  Mode:Nbr is  Slave  Priority: 2
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 33  sec
   Retrans timer interval: 5
   Neighbor is up for 00:11:15
```

```
  Authentication Sequence: [ 0 ]
```

NOTE

The DR priority on the interface is invalid after it is configured.

5. Restart OSPF processes.

   On each Switch, run the **reset ospf 1 process** command in the user view to restart the OSPF process.

6. Verify the configuration.

   # Check the status of OSPF neighbors.

```
[SwitchD] display ospf peer

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlanif10)'s neighbors
 Router ID: 1.1.1.1      Address: 192.168.1.1
   State: Full  Mode:Nbr is  Master  Priority: 100
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:07:19
   Authentication Sequence: [ 0 ]

 Router ID: 2.2.2.2      Address: 192.168.1.2
   State: 2-Way  Mode:Nbr is  Slave  Priority: 0
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:00
   Authentication Sequence: [ 0 ]

 Router ID: 3.3.3.3      Address: 192.168.1.3
   State: Full  Mode:Nbr is  Slave  Priority: 2
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 37  sec
   Retrans timer interval: 5
   Neighbor is up for 00:07:17
   Authentication Sequence: [ 0 ]
```

   # Check the status of an interface enabled with OSPF.

```
[SwitchA] display ospf interface

          OSPF Process 1 with Router ID 1.1.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     Broadcast    DR       1     100   192.168.1.1     192.168.1.3

[SwitchB] display ospf interface

          OSPF Process 1 with Router ID 2.2.2.2
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State      Cost  Pri   DR              BDR
 192.168.1.2     Broadcast    DROther  1       0     192.168.1.1     192.168.1.3
```

   All neighbors are in the full state. This indicates that SwitchA sets up neighbor relationships with all its neighbors. If the neighbor remains "2-Way", it indicates both of them are not DRs or BDRs. Thus, they need not exchange LSAs.

   All other neighbors are DR Others. This indicates that they are neither DRs nor BDRs.

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
router id 1.1.1.1
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
ospf dr-priority 100
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
router id 2.2.2.2
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
ospf dr-priority 0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
router id 3.3.3.3
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.3 255.255.255.0
ospf dr-priority 2
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
router id 4.4.4.4
```

```
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.4 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

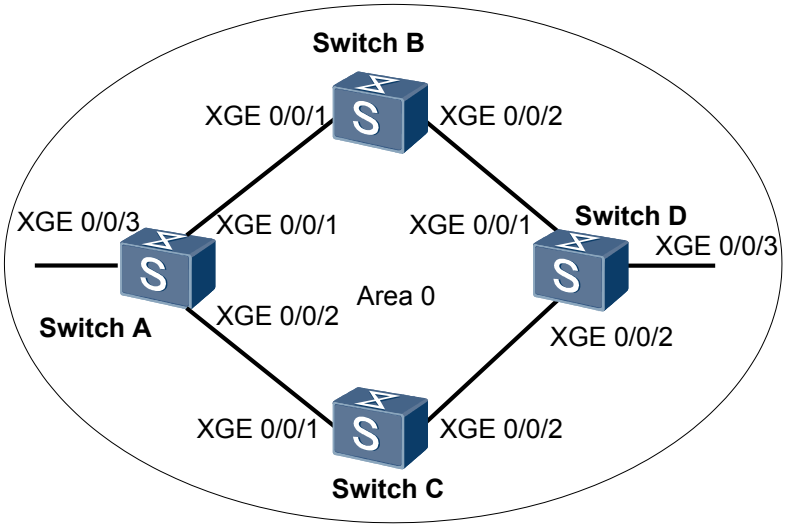
3.4.6 Example for Configuring OSPF Load Balancing

Networking Requirements

As shown in **Figure 3-12**:

- SwitchA, SwitchB, SwitchC, and SwitchD connect to each other through OSPF.
- SwitchA, SwitchB, SwitchC, and SwitchD belong to Area 0.
- Load balancing is performed between SwitchB and SwitchC. The traffic of SwitchA is sent to SwitchD by SwitchB and SwitchC.

Figure 3-12 Networking diagram for configuring OSPF load balancing



Device	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchA	XGE 0/0/2	VLANIF 20	10.1.2.1/24
SwitchA	XGE 0/0/3	VLANIF 50	172.16.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchB	XGE 0/0/2	VLANIF 30	192.168.0.1/24
SwitchC	XGE 0/0/1	VLANIF 20	10.1.2.2/24

SwitchC	XGE 0/0/2	VLANIF 40	192.168.1.1/24
SwitchD	XGE 0/0/1	VLANIF 30	192.168.0.2/24
SwitchD	XGE 0/0/2	VLANIF 40	192.168.1.2/24
SwitchD	XGE 0/0/3	VLANIF 60	172.17.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each Switch to implement interconnection.
2. Cancel load balancing and check the routing table.
3. (Optional) Set the preferences for equal-cost routes on SwitchA.

Data Preparation

To configure OSPF load balancing, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in **Figure 3-12**.
- The IP address of each interface is shown in **Figure 3-12**.
- The router ID of each Switch, the OSPF process ID, and the area to which each interface belongs are as follows:
  - The router ID of SwitchA is 1.1.1.1, the OSPF process ID is 1, and the network segments of Area 0 are 10.1.1.0/24, 10.1.2.0/24, and 172.16.1.0/24.
  - The router ID of SwitchB is 2.2.2.2, the OSPF process ID is 1, and the network segments of Area 0 are 10.1.1.0/24 and 192.168.0.0/24.
  - The router ID of SwitchC is 3.3.3.3, the OSPF process ID is 1, and the network segments of Area 0 are 10.1.2.0/24 and 192.168.1.0/24.
  - The router ID of SwitchD is 4.4.4.4, the OSPF process ID is 1, and the network segments of Area 0 are 172.17.1.0/24, 192.168.0.0/24, and 192.168.1.0/24.
  - The number of routes for load balancing on SwitchA is 1.
  - The preference of the equal-cost route of SwitchC is 1.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.
2. Assign an IP address to each interface.

   The configuration details are not mentioned here.
3. **3.4.2 Example for Configuring Basic OSPF Functions**.
4. Cancel load balancing on SwitchA.

   ```
   [SwitchA] ospf
   [SwitchA-ospf-1] maximum load-balancing 1
   [SwitchA-ospf-1] quit
   ```

   Check the routing table of SwitchA.

   ```
   [SwitchA] display ip routing-table
   ```

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13       Routes : 13

Destination/Mask       Proto   Pre   Cost    Flags   NextHop          Interface

      10.1.1.0/24      Direct  0     0       D       10.1.1.1         Vlanif10
       10.1.1.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
      10.1.1.2/32      Direct  0     0       D       10.1.1.2         Vlanif10
      10.1.2.0/24      Direct  0     0       D       10.1.2.1         Vlanif20
       10.1.2.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
      10.1.2.2/32      Direct  0     0       D       10.1.2.2         Vlanif20
     127.0.0.0/8       Direct  0      0       D        127.0.0.1
InLoopBack0
      127.0.0.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
     172.16.1.0/24      Direct  0     0       D       172.16.1.1       Vlanif50
     172.16.1.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
     172.17.1.0/24      OSPF    10     3       D       10.1.1.2         Vlanif10
    192.168.0.0/24      OSPF    10     2       D       10.1.1.2         Vlanif10
    192.168.1.0/24      OSPF    10     2       D       10.1.2.2         Vlanif20
```

As shown in the routing table, when the maximum number of the equal-cost routes is 1, the next hop to the destination network segment 172.17.1.0 is 10.1.1.2.

NOTE

In the preceding example, 10.1.1.2 is selected as the optimal next hop. This is because OSPF selects the next hop of the equal-cost route randomly.

5. Restore the default number of routes for load balancing on SwitchA.

```
[SwitchA] ospf
[SwitchA-ospf-1] undo maximum load-balancing
[SwitchA-ospf-1] quit
```

Check the routing table of SwitchA.

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11       Routes : 12
Destination/Mask       Proto   Pre   Cost  Flags     NextHop          Interface

      10.1.1.0/24      Direct  0     0       D       10.1.1.1         Vlanif10
       10.1.1.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
      10.1.2.0/24      Direct  0     0       D       10.1.2.1         Vlanif20
       10.1.2.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
      127.0.0.0/8       Direct  0      0       D        127.0.0.1
InLoopBack0
      127.0.0.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
     172.16.1.0/24      Direct  0     0       D       172.16.1.1       Vlanif50
     172.16.1.1/32      Direct  0      0       D        127.0.0.1
InLoopBack0
     172.17.1.0/24      OSPF    10     3       D       10.1.1.2         Vlanif10
                        OSPF    10     3       D       10.1.2.2         Vlanif2
     192.168.0.0/24     OSPF    10     2       D       10.1.1.2         Vlanif10
     192.168.1.0/24     OSPF    10     2       D       10.1.2.2         Vlanif20
```

As shown in the routing table, when the default setting of load balancing is restored, the next hops of SwitchA, that is, 10.1.1.2 (SwitchB) and 10.1.2.2 (SwitchC), become valid routes. This is because the default number of equal-cost routes is 4.

6. (Optional) Set the preferences for equal-cost routes on SwitchA.

   If you need not perform load balancing between SwitchB and SwitchC, set the preferences for equal-cost routes and specify the next hop.

```
[SwitchA] ospf
[SwitchA-ospf-1] nexthop 10.1.2.2 weight 1
[SwitchA-ospf-1] quit
```

   # Check the routing table of SwitchA.

```
[SwitchA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11       Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      10.1.1.0/24   Direct  0    0           D   10.1.1.1        Vlanif10
      10.1.1.1/32   Direct  0    0           D   127.0.0.1
InLoopBack0
      10.1.2.0/24   Direct  0    0           D   10.1.2.1        Vlanif20
      10.1.2.1/32   Direct  0    0           D   127.0.0.1
InLoopBack0
     127.0.0.0/8    Direct  0    0           D   127.0.0.1
InLoopBack0
     127.0.0.1/32   Direct  0    0           D   127.0.0.1
InLoopBack0
    172.16.1.0/24   Direct  0    0           D   172.16.1.1      Vlanif50
    172.16.1.1/32   Direct  0    0           D   127.0.0.1
InLoopBack0
    172.17.1.0/24   OSPF    10   3           D   10.1.2.2        Vlanif20
   192.168.0.0/24   OSPF    10   2           D   10.1.1.2        Vlanif10
   192.168.1.0/24   OSPF    10   2           D   10.1.2.2        Vlanif20
```

   As shown in the routing table, OSPF selects the next hop 10.1.2.2 as the unique optimal route. This is because the preference of the next hop 10.1.2.2 (SwitchC) is higher than that of the next hop 10.1.1.2 (SwitchB) after the preferences of the equal-cost routes are set.

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10 20 50
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif50
 ip address 172.16.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port trunk allow-pass vlan 50
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
```

```
#
return
```

- Configuration file of SwitchB

```
sysname SwitchB
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 30
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
#
interface Vlanif40
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 vlan batch 30 40 60
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
#
interface Vlanif40
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif60
 ip address 172.17.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/2
```

```
 port trunk allow-pass vlan 40
#
interface XGigabitEthernet0/0/3
 port trunk allow-pass vlan 60
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
```

3.5 OSPFv3 Configuration

By building Open Shortest Path First Version 3 (OSPFv3) networks, you can enable OSPFv3 to discover and calculate routes in ASs. OSPFv3 is applicable to a large-scale network that consists of hundreds of routers.

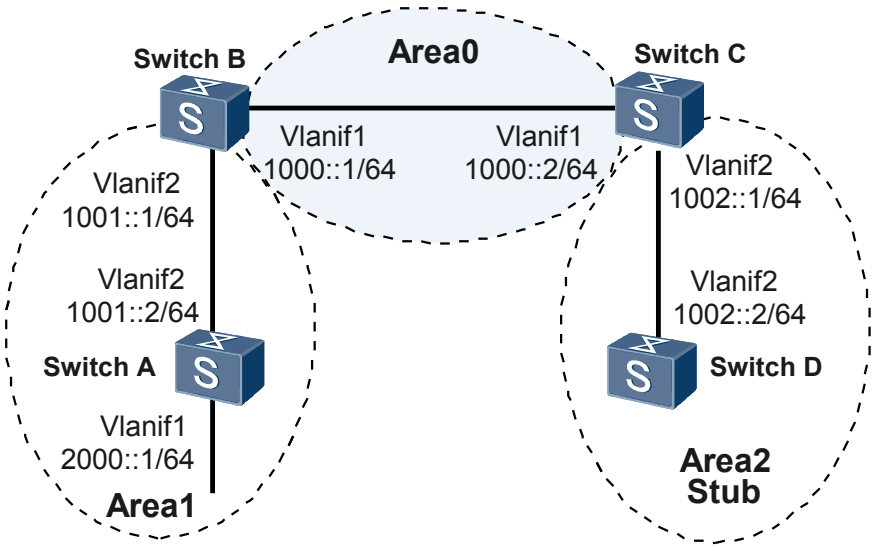
3.5.1 Example for Configuring OSPFv3 Areas

Networking Requirements

As shown in **Figure 3-13**, all Switches run OSPFv3. The entire autonomous system is divided into three areas. Switch-B and Switch-C serve as ABRs to forward the inter-area routes.

It is required that Area 2 be configured as a stub area to decrease the LSAs advertised to this area, without affecting route reachability.

Figure 3-13 Networking diagram for configuring OSPFv3 areas



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic OSPFv3 function on each Switch.
2. Configure Area 2 as a stub area and check the OSPFv3 routing table of Switch-D.
3. Configure Area 2 as a totally stub area and check the OSPFv3 routing table of Switch-D.

Data Preparation

To complete the configuration, you need the following data:

- Router ID of SwitchA as 1.1.1.1 of Area 1
- Router ID of SwitchB as 2.2.2.2 of Areas 0 and 1
- Router ID of SwitchC as 3.3.3.3 of Areas 0 and 2
- Router ID of SwitchD as 4.4.4.4 of Area 2

Procedure

Step 1 Assign an IPv6 address to each interface.

The details are not mentioned here.

Step 2 Configure basic OSPFv3 functions.

Configure SwitchA.

```
[SwitchA] ipv6
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlanif 1
[SwitchA-Vlanif1] ospfv3 1 area 1
[SwitchA-Vlanif1] quit
[SwitchA] interface vlanif 2
[SwitchA-Vlanif2] ospfv3 1 area 1
[SwitchA-Vlanif2] quit
```

Configure SwitchB.

```
[SwitchB] ipv6
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlanif 1
[SwitchB-Vlanif1] ospfv3 1 area 0
[SwitchB-Vlanif1] quit
[SwitchB] interface vlanif 2
[SwitchB-Vlanif2] ospfv3 1 area 1
[SwitchB-Vlanif2] quit
```

Configure SwitchC.

```
[SwitchC] ipv6
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlanif 1
[SwitchC-Vlanif1] ospfv3 1 area 0
[SwitchC-Vlanif1] quit
[SwitchC] interface vlanif 2
[SwitchC-Vlanif2] ospfv3 1 area 2
[SwitchC-Vlanif2] quit
```

Configure SwitchD.

```
[SwitchD] ipv6
```

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlanif 2
[SwitchD-Vlanif2] ospfv3 1 area 2
[SwitchD-Vlanif2] quit
```

Display the OSPFv3 neighbors of SwitchB.

```
[SwitchB] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
1.1.1.1           1   Full/ -          00:00:34    Vlanif2           0
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
3.3.3.3           1   Full/ -          00:00:32    Vlanif1           0
```

Display OSPFv3 neighbors of SwitchC.

```
[SwitchC] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
2.2.2.2           1   Full/ -          00:00:37    Vlanif1           0
OSPFv3 Area (0.0.0.2)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
4.4.4.4           1   Full/ -          00:00:33    Vlanif2           0
```

Display the OSPFv3 routing table of SwitchD.

```
[SwitchD] display ospfv3 routing
OSPFv3 Process (1)
   Destination                                    Metric
     Next-hop
  IA 1000::/64                                      2
           via FE80::1572:0:5EF4:1, Vlanif1
  IA 1001::/64                                      3
           via FE80::1572:0:5EF4:1, Vlanif1
     1002::/64                                      1
           directly-connected, Vlanif1
  IA 2000::/64                                      4
           via FE80::1572:0:5EF4:1, Vlanif1
```

Step 3 Configure stub areas.

Configure the stub area of SwitchD.

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] area 2
[SwitchD-ospfv3-1-area-0.0.0.2] stub
[SwitchD-ospfv3-1-area-0.0.0.2] quit
```

Configure the stub area of SwitchC, and set the cost of the default route advertised to the stub area to 10.

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
[SwitchC-ospfv3-1-area-0.0.0.2] quit
```

Display the OSPFv3 routing table of SwitchD, and you can view a new default route in the routing table. Its cost is the sum of the cost of the directly connected routes and the configured cost.

```
[SwitchD] display ospfv3 routing
OSPFv3 Process (1)
   Destination                                    Metric
```

```
   Next-hop
IA ::/0                                          11
         via FE80::1572:0:5EF4:1, Vlanif1
IA 1000::/64                                     2
         via FE80::1572:0:5EF4:1, Vlanif1
IA 1001::/64                                     3
         via FE80::1572:0:5EF4:1, Vlanif1
   1002::/64                                     1
         directly-connected, Vlanif1
IA 2000::/64                                     4
         via FE80::1572:0:5EF4:1, Vlanif1
```

Step 4 Configure totally stub areas.

Configure SwitchC and configure Area 2 as a totally stub area.

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
[SwitchC-ospfv3-1-area-0.0.0.2] quit
```

Step 5 Verify the configuration.

Display the OSPFv3 routing table of SwitchD, and you can view that the entries in the routing table decrease; other non-directly connected routes are suppressed; only the default route is reserved.

```
[SwitchD] display ospfv3 routing
OSPFv3 Process (1)
   Destination                                   Metric
     Next-hop
  IA ::/0                                        11
           via FE80::1572:0:5EF4:1, Vlanif1
     1002::/64                                   1
           directly-connected, Vlanif1
```

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 ipv6
#
interface Vlanif1
 ipv6 address 2000::1/64
 ospfv3 1 area 0.0.0.1
#
interface Vlanif2
ipv6 address 1001::2/64
 ospfv3 1 area 0.0.0.1
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.1
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 ipv6
#
interface Vlanif1
```

```
ipv6 address 1000::1/64
 ospfv3 1 area 0.0.0.0
#
interface Vlanif2
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.1
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
 area 0.0.0.1
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 ipv6
#
interface Vlanif1
ipv6 address 1000::2/64
 ospfv3 1 area 0.0.0.0
#
interface Vlanif2
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.2
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
 area 0.0.0.2
  stub no-summary
  default-cost 10
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 ipv6
#
interface Vlanif2
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.2
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.2
  stub
#
return
```

3.6 IS-IS Configuration

This chapter describes the basic principle of IS-IS and procedures for configuring IS-IS, and provides configuration examples.

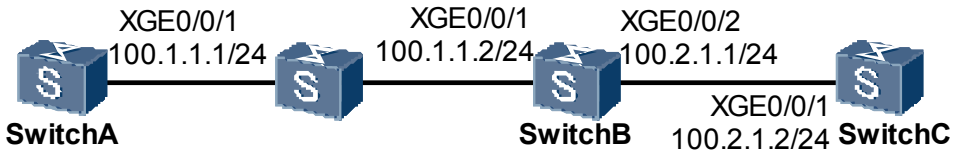
3.6.1 Example for Configuring Static BFD for IS-IS

Networking Requirements

As show in **Figure 3-14**:

- A Layer 2 switch exists between Switch A and Switch B.
- Switch A, Switch B and Switch C run IS-IS.
- BFD is configured to detect the IS-IS neighbor relationship between Switch A and Switch B. When the link between Switch A and Switch B is faulty, BFD can fast detect the default and report it to IS-IS.

Figure 3-14 Networking diagram for configuring static BFD for IS-IS



Switch	Interface	VLANIF interface	IP address
SwitchA	XGE0/0/1	VLANIF 10	100.1.1.1/24
SwitchB	XGE0/0/1	VLANIF 20	100.1.1.2/24
SwitchB	XGE0/0/2	VLANIF 30	100.2.1.1/24
SwitchC	XGE0/0/1	VLANIF 30	100.2.1.2/24

NOTE

BFD for IS-IS cannot be used to detect the multi-hops link between Switch A and Switch C, because the IS-IS neighbor relationship cannot be established between Switch A and Switch C.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each switch.
2. Enable BFD on Switch A and Switch B.

Data Preparation

To complete the configuration, you need the following data:

- IS-IS process ID
- Area addresses of Switch A, Switch B, and Switch C
- Levels of Switch A, Switch B, and Switch C
- Name of the BFD session set up between Switch A and Switch B and the peer IP address to be detected
- Local and remote discriminators of the BFD session set up between Switch A and Switch B

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname SwitchA
```

```
[SwitchA] vlan batch 10
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Step 2 Configure an IP address for each VLANIF interface.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 100.1.1.1 24
[SwitchA-Vlanif10] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Step 3 Configuration basic IS-IS functions.

Configure Switch A.

```
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-2
[SwitchA-isis-1] network-entity aa.1111.1111.1111.00
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis enable 1
[SwitchA-Vlanif10] quit
```

Configure Switch B.

```
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-2
[SwitchB-isis-1] network-entity aa.2222.2222.2222.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] isis enable 1
[SwitchB-Vlanif20] quit
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] isis enable 1
[SwitchB-Vlanif30] quit
```

Configure Switch C.

```
[SwitchC] isis 1
[SwitchC-isis-1] is-level level-2
[SwitchC-isis-1] network-entity aa.3333.3333.3333.00
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 30
[SwitchC-Vlanif30] isis enable 1
[SwitchC-Vlanif30] quit
```

After the preceding configurations, you can view that the neighbor relationship is established between Switch A and Switch B.

```
[SwitchA] display isis peer
                          Peer information for ISIS(1)
                          ----------------------------
  System Id    Interface         Circuit Id       State HoldTime Type     PRI
2222.2222.2222 Vlanif10             001              Up   23s      L2       64
```

The IS-IS routing table of Switch A has entries to Switch B and Switch C.

```
[SwitchA] display isis route
                         Route information for ISIS(1)
                         ----------------------------
                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------
```

```
 IPV4 Destination    IntCost   ExtCost ExitInterface   NextHop      Flags
------------------------------------------------------------------------------
 100.1.1.0/24        10         NULL    Vlanif10        Direct       D/-/L/-
 100.2.1.0/24        20         NULL    Vlanif10        100.1.1.2    A/-/L/-
      Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
```

Step 4 Configure BFD.

Enable BFD on Switch A and configure a BFD session.

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atob bind peer-ip 100.1.1.2 interface vlanif 10
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

Enable BFD on Switch B and configure a BFD session.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] bfd btoa bind peer-ip 100.1.1.1 interface vlanif 20
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

After the preceding configurations, you can view that the status of the BFD session is Up when the **display bfd session** command is used on Switch A or Switch B.

The display on Switch A is as follows:

```
[SwitchA] display bfd session all
--------------------------------------------------------------------------------
Local Dis  Remote Dis  Peer IP Address  Interface Name       State    Type
--------------------------------------------------------------------------------
1           2          100.1.1.2        Vlanif10              Up       S_IP
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

Step 5 Enable IS-IS fast sense.

Configure Switch A.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis bfd static
[SwitchA-Vlanif10] quit
```

Configure Switch B.

```
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] isis bfd static
[SwitchB-Vlanif20] quit
```

Step 6 Verify the configuration.

Enable the debugging on Switch A and output information to the VTY tunnel.

```
[SwitchA] info-center source bfd channel 1 log level debugging state on
[SwitchA] quit
<SwitchA> debugging isis circuit-information
<SwitchA> terminal debugging
<SwitchA> terminal logging
<SwitchA> terminal monitor
```

Run the **shutdown** command on Vlanif20 of Switch B to simulate a link fault.

```
[SwitchB-Vlanif20] shutdown
```

On Switch A, the following log information and debugging information are displayed. It indicates that IS-IS deletes the neighbor relationship with Switch B according to the fault reported by BFD.

```
Sep 12 2007 11:32:18 RT2 %%01ISIS/4/PEER_DOWN_BFDDOWN(l): IS-IS process id 1 nei
ghbor 2222.2222.2222 is down on the interface GE1/0/0 because BFD node is Down.
 The last Hello packet is received at 11:32:10. The maximum interval for sending
 Hello packets is 9247. The local router sends 426 Hello packets and receives 61
 Hello packets. The Hello packet type is Lan Level-2.
*0.481363988 RT2 ISIS/6/ISIS:
 ISIS-1-FastSense: Deleting Neighbour by IP Address 100.1.1.2 On Vlanif20(IS01_1048)
```

Run the **display isis route** command or the **display isis peer** command on Switch A, no information is displayed. This indicates that the IS-IS neighbor relationship between Switch A and Switch B is deleted.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 10
#
 info-center source BFD channel 1 log level debugging
#
bfd
#
isis 1
 is-level level-2
 network-entity aa.1111.1111.1111.00
#
interface Vlanif10
 ip address 100.1.1.1 255.255.255.0
 isis enable 1
 isis bfd static
#
bfd atob bind peer-ip 100.1.1.2 interface Vlanif10
 discriminator local 1
 discriminator remote 2
 commit
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 20 30
#
bfd
#
isis 1
 is-level level-2
 network-entity aa.2222.2222.2222.00
#
interface Vlanif20
 ip address 100.1.1.2 255.255.255.0
 isis enable 1
 isis bfd static
#
```

```
interface Vlanif30
 ip address 100.2.1.1 255.255.255.0
 isis enable 1
#
bfd btoa bind peer-ip 100.1.1.1 interface Vlanif20
 discriminator local 2
 discriminator remote 1
 commit
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 30
#
isis 1
 is-level level-2
 network-entity aa.3333.3333.3333.00
#
interface Vlanif30
 ip address 100.2.1.2 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
return
```

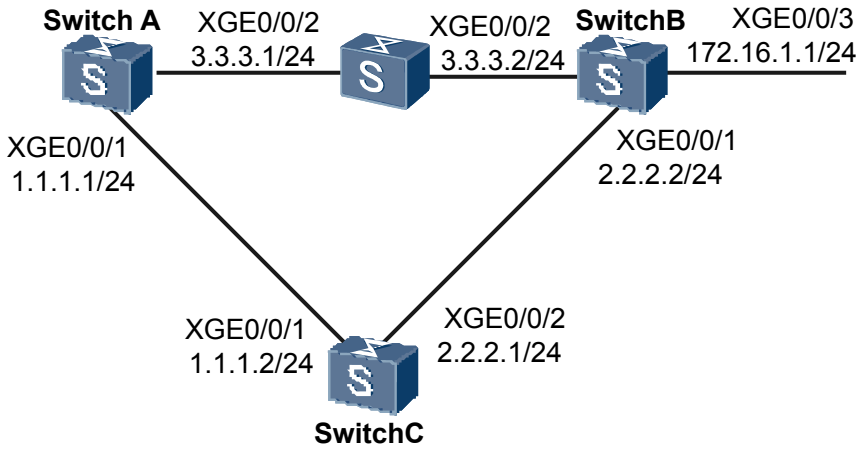
3.6.2 Example for Configuring Dynamic BFD for IS-IS

Networking Requirements

As shown in **Figure 3-15**, it is required as follows:

- Run IS-IS on Switch A, Switch B, and Switch C.
- Enable BFD of the IS-IS process on Switch A, Switch B, and Switch C.
- Traffic is transmitted on the active link Switch A → Switch B. The link Switch A → Switch B → Switch C acts as the standby link.
- Enable BFD of the interface on the link between Switch A and Switch B. When the link between Switch A and Switch B fails, BFD can quickly detect the fault and notify IS-IS of the fault; therefore, the traffic is transmitted on the standby link.

Figure 3-15 Networking diagram for configuring the dynamic BFD



Switch	Interface	VLANIF interface	IP address
Switch A	XGE0/0/1	VLANIF 10	1.1.1.1/24
Switch A	XGE0/0/2	VLANIF 20	3.3.3.1/24
Switch B	XGE0/0/1	VLANIF 50	2.2.2.2/24
Switch B	XGE0/0/2	VLANIF 30	3.3.3.2/24
Switch B	XGE0/0/3	VLANIF 40	172.16.1.1/24
Switch C	XGE0/0/2	VLANIF 50	2.2.2.1/24
Switch C	XGE0/0/1	VLANIF 10	1.1.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IS-IS on each switch and ensure the connectivity of the switches
2. Set the interface cost of IS-IS to control the route selection of the switches.
3. Enable global BFD.
4. Enable the BFD detection mechanism of the IS-IS process on Switch A, Switch B, and Switch C.
5. Enable the BFD detection mechanism of the interfaces on Switch A and Switch B.

Data Preparation

To complete the configuration, you need the following data:

- Process ID of IS-IS
- Area numbers of Switch A, Switch B, and Switch C
- Interface cost of Switch A, Switch B and Switch C
- Interface number and type number of BFD enabled on Switch A and Switch B

- Minimum interval for sending the BFD packets, minimum interval for receiving the BFD packets, and local detection multiple on Switch A and Switch B

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname Switch A
[SwitchA] vlan batch 10 20
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid pvid vlan 20
[SwitchA-XGigabitEthernet0/0/2] port hybrid untagged vlan 20
[SwitchA-XGigabitEthernet0/0/2] quit
```

The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA, and are not mentioned here.

Step 2 Assign an IP address to each VLANIF interface.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 1.1.1.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 3.3.3.1 24
[SwitchA-Vlanif20] quit
```

The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA, and are not mentioned here.

Step 3 Configure the basic IS-IS functions.

Configure Switch A.

```
[SwitchA] isis
[SwitchA-isis-1] is-level level-2
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis enable 1
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] isis enable 1
[SwitchA-Vlanif20] quit
```

Configure Switch B.

```
[SwitchB] isis
[SwitchB-isis-1] is-level level-2
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] isis enable 1
[SwitchB-Vlanif50] quit
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] isis enable 1
[SwitchB-Vlanif30] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] isis enable 1
[SwitchB-Vlanif40] quit
```

Configure Switch C.

```
[SwitchC] isis
```

```
[SwitchC-isis-1] is-level level-2
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] isis enable 1
[SwitchC-Vlanif10] quit
[SwitchC] interface vlanif 50
[SwitchC-Vlanif50] isis enable 1
[SwitchC-Vlanif50] quit
```

After the preceding configurations are complete, use the **display isis peer** command. You can view that the neighboring relationship is set up between Switch A and Switch B, and that between Switch A and Switch C. Take the configuration on Switch A as an example:

```
[SwitchA] display isis peer
                        Peer information for ISIS(1)
                        ---------------------------
  System Id     Interface          Circuit Id       State HoldTime Type     PRI
0000.0000.0002  Vlanif20           0000.0000.0002.01 Up   9s       L2       64
0000.0000.0003  Vlanif10           0000.0000.0001.02 Up   21s      L2       64
Total Peer(s): 2
```

The switches have learned routes of each other. Take the routing table of Switch A as an example:

```
[SwitchA] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 9
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
        1.1.1.0/24  Direct 0    0           D  1.1.1.1        Vlanif10
        1.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
        2.2.2.0/24  ISIS   15   20          D  1.1.1.2         Vlanif10
        3.3.3.0/24  Direct 0    0           D  3.3.3.1         Vlanif20
        3.3.3.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
  172.16.1.0/24  ISIS   15   20          D  3.3.3.2         Vlanif20
```

As shown in the routing table, the next hop address of the route to 172.16.1.0/24 is 3.3.3.2 and traffic is transmitted on the active link from Switch A to Switch B.

Step 4 Set the interface cost.

Configure Switch A.

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] isis cost 5
[SwitchA-Vlanif20] quit
```

Configure Switch B.

```
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] isis cost 5
[SwitchB-Vlanif30] quit
```

Step 5 Configure BFD of the IS-IS process.

Enable BFD of the IS-IS process on Switch A.

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] isis
[SwitchA-isis-1] bfd all-interfaces enable
[SwitchA-isis-1] quit
```

Enable BFD of the IS-IS process on Switch B.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] isis
[SwitchB-isis-1] bfd all-interfaces enable
[SwitchB-isis-1] quit
```

Enable BFD of the IS-IS process on Switch C.

```
[SwitchC] bfd
[SwitchC-bfd] quit
[SwitchC] isis
[SwitchC-isis-1] bfd all-interfaces enable
[SwitchC-isis-1] quit
```

After the preceding configurations are complete, run the **display isis bfd session all** command on Switch A, Switch B, or Switch C. You can view that the status of BFD is Up.

Take the display of Switch A as an example:

```
[SwitchA] display isis bfd session all
                     BFD session information for ISIS(1)
                     ------------------------------------
Peer System ID : 0000.0000.0002        Interface : Vlanif20
TX : 100         BFD State : up      Peer IP Address : 3.3.3.2
RX : 100          LocDis : 8193       Local IP Address: 1.1.1.1
Multiplier : 3     RemDis : 8192       Type : L2
Diag : No diagnostic information
Peer System ID : 0000.0000.0003        Interface : Vlanif10
Multiplier : 3     RemDis : 8192       Type : L2
Diag : No diagnostic information
```

From the preceding display, you can view that the status of the BFD session between Switch A and Switch B and that between Switch A and Switch C are Up.

Step 6 Configure BFD of the interfaces.

Configure BFD on Vlanif20 of Switch A, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiple to 4.

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] isis bfd enable
[SwitchA-Vlanif20] isis bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
[SwitchA-Vlanif20] quit
```

Configure BFD on Vlanif20 of Switch B, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiple to 4.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] isis bfd enable
[SwitchB-Vlanif30] isis bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
[SwitchB-Vlanif30] quit
```

After the preceding configurations are complete, run the **display isis bfd session all** command on Switch A or Switch B. You can view that the parameters of the BFD have taken effect. Take the display of Switch B as an example:

```
[SwitchB] display isis bfd session all
                     BFD session information for ISIS(1)
                     ------------------------------------
Peer System ID : 0000.0000.0001        Interface : Vlanif30
TX : 100           BFD State : up      Peer IP Address : 3.3.3.1
```

```
RX : 100           LocDis : 8192       Local IP Address: 3.3.3.2
Multiplier : 4     RemDis : 8192       Type : L2
Diag : No diagnostic information
Peer System ID : 0000.0000.0003        Interface : Vlanif50
TX : 100           BFD State : up      Peer IP Address : 2.2.2.1
RX : 100           LocDis : 8192       Local IP Address: 2.2.2.2
Multiplier : 3     RemDis : 8193       Type : L2
Diag : No diagnostic information
```

Step 7 Verify the configuration.

Run the **shutdown** command on Vlanif30 of Switch B to simulate the active link failure.

```
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] shutdown
```

Step 8 # Display the routing table on Switch A.

```
[SwitchA] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
        1.1.1.0/24  Direct 0    0           D  1.1.1.1         Vlanif10
        1.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
        2.2.2.0/24  ISIS   15   20          D  1.1.1.2         Vlanif10
        3.3.3.0/24  Direct 0    0           D  3.3.3.1         Vlanif10
        3.3.3.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
     172.16.1.0/24  ISIS   15   20          D  1.1.1.2         Vlanif10
```

As shown in the routing table, the standby link Switch A → Switch C → Switch B takes effect after the active link fails. The next hop address of the route to 172.16.1.0/24 becomes 1.1.1.2.

Run the **display isis bfd session all** command on Switch A. You can view the status of the BFD session is Up between Switch A and Switch C.

```
[SwitchA] display isis bfd session all
                      BFD session information for ISIS(1)
                      -----------------------------------
Peer System ID : 0000.0000.0003        Interface : Vlanif10
TX : 100           BFD State : up      Peer IP Address : 1.1.1.2
RX : 100           LocDis : 8192       Local IP Address: 1.1.1.1
Multiplier : 3     RemDis : 8192       Type : L2
Diag : No diagnostic information
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 10 20
#
 bfd
#
isis 1
 is-level level-2
 bfd all-interfaces enable
 network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 1.1.1.1 255.255.255.0
 isis enable 1
```

```
#
interface Vlanif20
 ip address 3.3.3.1 255.255.255.0
 isis enable 1
 isis cost 5
 isis bfd enable
 isis bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 30 40 50
#
 bfd
#
isis 1
 is-level level-2
 bfd all-interfaces enable
 network-entity 10.0000.0000.0002.00
#
interface Vlanif50
 ip address 2.2.2.2 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 3.3.3.2 255.255.255.0
 isis enable 1
 isis cost 5
 isis bfd enable
 isis bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 10 50
#
 bfd
#
isis 1
 is-level level-2
```

```
 bfd all-interfaces enable
 network-entity 10.0000.0000.0003.00
#
interface Vlanif10
undo shutdown
 ip address 1.1.1.2 255.255.255.0
 isis enable 1
#
interface Vlanif50
undo shutdown
 ip address 2.2.2.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
return
```

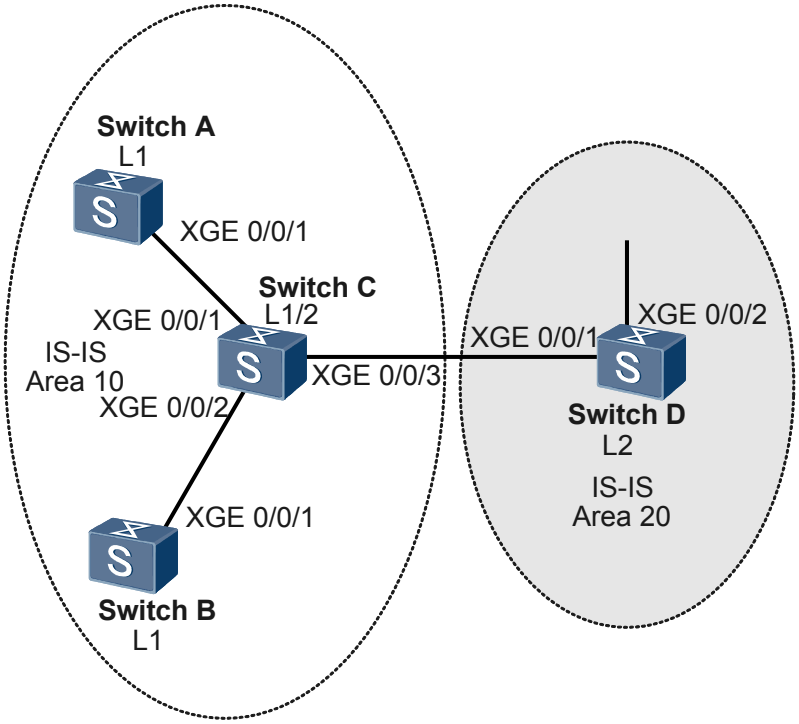
3.6.3 Example for Configuring Basic IS-IS Functions

Networking Requirements

As shown in **Figure 3-16**:

- SwitchA, SwitchB, SwitchC, and SwitchD belong to the same domain. The IS-IS routing protocol runs on these four Switchs to ensure connectivity on an IP network.
- The areas IDs of SwitchA, SwitchB, and SwitchC are all 10, and the area ID of SwitchD is 20.
- SwitchA and SwitchB are Level-1 Switchs. SwitchC is the Level-1-2 Switch. SwitchD is the Level-2 Switch.

Figure 3-16 Networking diagram for configuring basic IS-IS functions



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchB	XGE 0/0/1	VLANIF 20	10.1.2.2/24
SwitchC	XGE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchC	XGE 0/0/2	VLANIF 20	10.1.2.1/24
SwitchC	XGE 0/0/3	VLANIF 30	192.168.0.1/24
SwitchD	XGE 0/0/1	VLANIF 30	192.168.0.2/24
SwitchD	XGE 0/0/2	VLANIF 40	172.16.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the VLANs to which the physical interfaces belong.
2. Assign IP addresses to VLANIF interfaces.
3. Run the IS-IS progress on each Switch, specify the network entity, and configure the level.
4. Check the IS-IS database and routing table of each Switch.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in **Figure 3-16**

- IP address of each VLANIF interface, as shown in **Figure 3-16**
- System ID, level, and area ID of each Switch
  - SwitchA: The system ID is 0000.0000.0001; the area ID is 10; the level is Level-1.
  - SwitchB: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-1.
  - SwitchC: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-1-2.
  - SwitchD: The system ID is 0000.0000.0004; the area ID is 20; the level is Level-2.

Configuration Procedure

1. Configure the IDs of the VLANs to which the interfaces belong.

   The configuration details are not mentioned.
2. Assign IP addresses to VLANIF interfaces.

   The configuration details are not mentioned.
3. Run the IS-IS progress on each Switch, specify the network entity, and configure the level.

   # Configure SwitchA.

   ```
   [SwitchA] isis 1
   [SwitchA-isis-1] is-level level-1
   [SwitchA-isis-1] network-entity 10.0000.0000.0001.00
   [SwitchA-isis-1] quit
   ```

   # Configure SwitchB.

   ```
   [SwitchB] isis 1
   [SwitchB-isis-1] is-level level-1
   [SwitchB-isis-1] network-entity 10.0000.0000.0002.00
   [SwitchB-isis-1] quit
   ```

   # Configure SwitchC.

   ```
   [SwitchC] isis 1
   [SwitchC-isis-1] network-entity 10.0000.0000.0003.00
   [SwitchC-isis-1] quit
   ```

   # Configure SwitchD.

   ```
   [SwitchD] isis 1
   [SwitchD-isis-1] is-level level-2
   [SwitchD-isis-1] network-entity 20.0000.0000.0004.00
   [SwitchD-isis-1] quit
   ```
4. Enable the IS-IS progress on each interface and enable IS-IS small-hello.

   # Configure SwitchA.

   ```
   [SwitchA] interface vlanif 10
   [SwitchA-Vlanif10] isis enable 1
   [SwitchA-Vlanif10] quit
   ```

   # Configure SwitchB.

   ```
   [SwitchB] interface vlanif 20
   [SwitchB-Vlanif20] isis enable 1
   [SwitchB-Vlanif20] quit
   ```

   # Configure SwitchC.

   ```
   [SwitchC] interface vlanif 10
   [SwitchC-Vlanif10] isis enable 1
   [SwitchC-Vlanif10] quit
   [SwitchC] interface vlanif 20
   [SwitchC-Vlanif20] isis enable 1
   [SwitchC-Vlanif20] quit
   [SwitchC] interface vlanif 30
   [SwitchC-Vlanif30] isis enable 1
   [SwitchC-Vlanif30] quit
   ```

   # Configure SwitchD.

```
[SwitchD] interface vlanif 30
[SwitchD-Vlanif30] isis enable 1
[SwitchD-Vlanif30] quit
[SwitchD] interface vlanif 40
[SwitchD-Vlanif40] isis enable 1
[SwitchD-Vlanif40] quit
```

5. Verify the configuration.

   # Display the IS-IS LSDB of each Switch.

```
[SwitchA] display isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime     Length  ATT/P/
OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x00000006   0xbf7d        649          68       0/0/0
0000.0000.0002.00-00  0x00000003   0xef4d        545          68       0/0/0
0000.0000.0003.00-00  0x00000008   0x3340        582          111      1/0/0
0000.0000.0003.01-00  0x00000004   0xa7dd        582          55       0/0/0
0000.0000.0003.02-00  0x00000002   0xc0c4        524          55       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
[SwitchB] display isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime     Length  ATT/P/
OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xbf7d        642          68       0/0/0
0000.0000.0002.00-00* 0x00000003   0xef4d        538          68       0/0/0
0000.0000.0003.00-00  0x00000008   0x3340        574          111      1/0/0
0000.0000.0003.01-00  0x00000004   0xa7dd        582          55       0/0/0
0000.0000.0003.02-00  0x00000002   0xc0c4        524          55       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
[SwitchC] display isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime     Length  ATT/P/
OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xbf7d        638          68       0/0/0
0000.0000.0002.00-00  0x00000003   0xef4d        533          68       0/0/0
0000.0000.0003.00-00* 0x00000008   0x3340        569          111      1/0/0
0000.0000.0003.01-00* 0x00000005   0xa7dd        569          55       0/0/0
0000.0000.0003.02-00* 0x00000003   0xc0c4        569          55       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload

                        Level-2 Link State Database

LSPID                 Seq Num      Checksum      Holdtime     Length  ATT/P/
OL
-------------------------------------------------------------------------------
```

```
0000.0000.0003.00-00*   0x00000008   0x55bb        650           100      0/0/0
0000.0000.0003.03-00*   0x00000003   0xef91        650           55       0/0/0
0000.0000.0004.00-00    0x00000005   0x651         629           84       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
[SwitchD] display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-2 Link State Database

LSPID                   Seq Num      Checksum      Holdtime     Length  ATT/P/
OL
-------------------------------------------------------------------------------
0000.0000.0003.00-00    0x00000008   0x55bb        644           100      0/0/0
0000.0000.0003.03-00    0x00000003   0xef91        644           55       0/0/0
0000.0000.0004.00-00*   0x00000005   0x651         624           84       0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
          ATT-Attached, P-Partition, OL-Overload
```

Display the IS-IS routing information of each Switch. A default route must be available in the routing table of the Level-1 Switch and the next hop is a Level-1-2 Switch. The routing table of the Level-2 Switch must contain all Level-1 and Level-2 routes.

```
[SwitchA] display isis route

                         Route information for ISIS(1)
                         ------------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
0.0.0.0/0             10         NULL      Vlanif10        10.1.1.1
A/-/-/-
 10.1.1.0/24          10         NULL      Vlanif10        Direct          D/-/
L/-
 10.1.2.0/24          20         NULL      Vlanif10        10.1.1.1
A/-/-/-
 192.168.0.0/24       20         NULL      Vlanif10        10.1.1.1
A/-/-/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchC] display isis route

                         Route information for ISIS(1)
                         ------------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 10.1.1.0/24          10         NULL      Vlanif10        Direct          D/-/
L/-
 10.1.2.0/24          10         NULL      Vlanif20        Direct          D/-/
L/-
 192.168.0.0/24       10         NULL      Vlanif30        Direct          D/-/
L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set


                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------
```

```
 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop         Flags
------------------------------------------------------------------------------
 10.1.1.0/24          10         NULL      Vlanif10        Direct          D/-/
L/-
 10.1.2.0/24          10         NULL      Vlanif20        Direct          D/-/
L/-
 192.168.0.0/24       10         NULL      Vlanif30        Direct          D/-/
L/-
 172.16.0.0/16        20         NULL      Vlanif40        192.168.0.2
A/-/-/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchD] display isis route

                        Route information for ISIS(1)
                        -----------------------------

                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------
 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop         Flags
------------------------------------------------------------------------------
 192.168.0.0/24       10         NULL      Vlanif30        Direct          D/-/
L/-
 10.1.1.0/24          20         NULL      Vlanif30        192.168.0.1
A/-/-/-
 10.1.2.0/24          20         NULL      Vlanif30        192.168.0.1
A/-/-/-
 172.16.0.0/16          10       NULL      Vlanif40        Direct
A/-/-/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10
#
isis 1
 is-level level-1
network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 20
#
isis 1
 is-level level-1
network-entity 10.0000.0000.0002.00
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
```

```
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 vlan batch 10 20 30
#
isis 1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 vlan batch 30 40
#
isis 1
 is-level level-2
network-entity 20.0000.0000.0004.00
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 172.16.1.1 255.255.0.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
Return
```

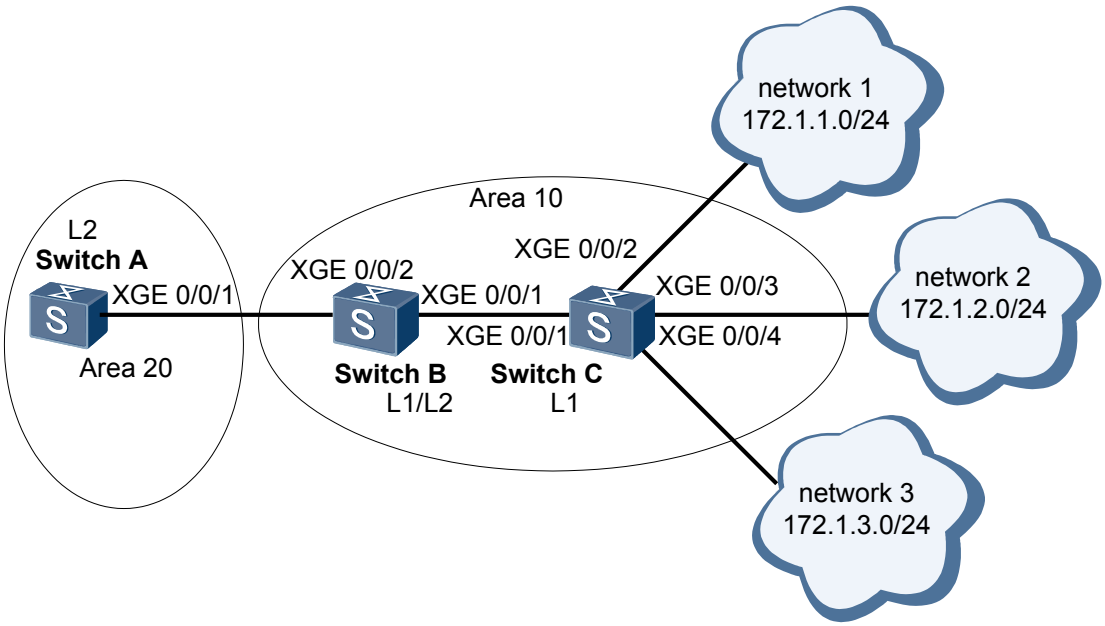
3.6.4 Example for Configuring IS-IS Route Aggregation

Networking Requirements

As shown in **Figure 3-17**:

- SwitchA, SwitchB, and SwitchC are interconnected by running the IS-IS protocol.
- SwitchA belongs to Area 20. SwitchB and SwitchC belong to Area 10.
- SwitchA is a Level-2 Switch. SwitchB is a Level-1-2 Switch. SwitchC is a Level-1 Switch.
- The addresses in Area 10 can be aggregated as 172.1.0.0/16.

Figure 3-17 Networking diagram for configuring IS-IS route convergence



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 50	172.2.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	172.1.4.2/24
SwitchB	XGE 0/0/2	VLANIF 50	172.2.1.2/24
SwitchC	XGE 0/0/1	VLANIF 10	172.1.4.1/24
SwitchC	XGE 0/0/2	VLANIF 20	172.1.1.1/24
SwitchC	XGE 0/0/3	VLANIF 30	172.1.2.1/24
SwitchC	XGE 0/0/4	VLANIF 40	172.1.3.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each Switch so that the Switches can be interconnected.
2. Check the IS-IS routing table of SwitchA.
3. Configure route convergence on SwitchB.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in **Figure 3-17**
- IP address of each VLANIF interface, as shown in **Figure 3-17**
- System ID, level, and area ID of each Switch
  - SwitchA: The system ID is 0000.0000.0001; the area ID is 20; the level is Level-2.
  - SwitchB: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-1-2.
  - SwitchC: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-1.

Configuration Procedure

1. Configure the VLAN ID of each physical interface.

   The configuration details are not mentioned here.
2. Assign IP addresses to VLANIF interfaces.

   The configuration details are not mentioned here.
3. Configure basic IS-IS functions.

   # Configure SwitchA.

```
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-2
[SwitchA-isis-1] network-entity 20.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 50
[SwitchA-Vlanif50] isis enable 1
[SwitchA-Vlanif50] quit
```

   # Configure SwitchB.

```
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] isis enable 1
[SwitchB-Vlanif10] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] isis enable 1
[SwitchB-Vlanif50] quit
```

   # Configure SwitchC.

```
[SwitchC] isis 1
[SwitchC-isis-1] is-level level-1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] isis enable 1
[SwitchC-Vlanif10] quit
```

   The configurations of the VLANIF 20, VLANIF30, and VLANIF 40 interfaces are the same as the configuration of the VLANIF 10 interface.
4. Check the IS-IS routing table of SwitchA.

```
[SwitchA]display isis route
```

```
                         Route information for ISIS(1)
                         ----------------------------

                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------

 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 172.1.1.0/24         20         NULL      Vlanif50        172.2.1.2
A/-/-/-
 172.1.2.0/24         20         NULL      Vlanif50        172.2.1.2
A/-/-/-
 172.1.3.0/24         20         NULL      Vlanif50        172.2.1.2
A/-/-/-
 172.1.4.0/24         20         NULL      Vlanif50        172.2.1.2
A/-/-/-
 172.2.1.0/24         10         NULL      Vlanif50        Direct          D/-/
L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

5. Configure route convergence on SwitchB.

   # Aggregate 172.1.1.0/24, 172.1.2.0/24, 172.1.3.0./24, and 172.1.4.0/24 as 172.1.0.0/16 on SwitchB.

```
[SwitchB] isis 1
[SwitchB-isis-1] summary 172.1.0.0 255.255.0.0 level-1-2
[SwitchB-isis-1] quit
```

6. Verify the configuration.

   # Display the routing table of SwitchA, and you can find that 172.1.1.0/24, 172.1.2.0/24, 172.1.3.0/24, and 172.1.4.0/24 are aggregated as 172.1.0.0/16.

```
[SwitchA] display isis route

                         Route information for ISIS(1)
                         ----------------------------

                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------

 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 172.1.0.0/16         20         NULL      Vlanif50        172.2.1.2
A/-/-/-
 172.2.1.0/24         10         NULL      Vlanif50        Direct          D/-/
L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set
```

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 50
#
isis 1
 is-level level-2
network-entity 20.0000.0000.0001.00
#
interface Vlanif50
 ip address 172.2.1.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 50
```

```
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 10 50
#
isis 1
network-entity 10.0000.0000.0002.00
 summary 172.1.0.0 255.255.0.0 level-1-2
#
interface Vlanif10
 ip address 172.1.4.2 255.255.255.0
 isis enable 1
#
interface Vlanif50
 ip address 172.2.1.2 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 vlan batch 10 20 30 40
#
isis 1
is-level level-1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
 ip address 172.1.4.1 255.255.255.0
 isis enable 1
#
interface Vlanif20
 ip address 172.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 172.1.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 172.1.3.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/4
```

```
 port link-type trunk
 port trunk allow-pass vlan 40
#
return
```

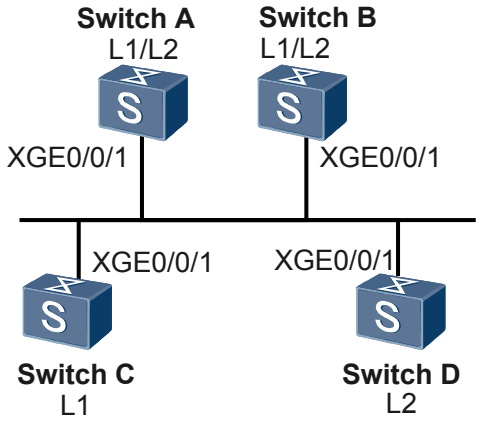
3.6.5 Example for Configuring the DIS Election of IS-IS

Networking Requirements

As shown in **Figure 3-18**:

- SwitchA, SwitchB, SwitchC, and SwitchD are interconnected by running the IS-IS protocol.
- SwitchA, SwitchB, SwitchC, and SwitchD belong to Area 10.
- SwitchA and SwitchB are Level-1-2 S-switchs. SwitchC is the Level-1 Switch. SwitchD is the Level-2 Switch.
- It is required to change the DIS priority of the interface to configure SwitchA to a Level-1-2 DIS.

Figure 3-18 Networking diagram for configuring the DIS election of IS-IS



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchC	XGE 0/0/1	VLANIF 10	10.1.1.3/24
SwitchD	XGE 0/0/1	VLANIF 10	10.1.1.4/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each Switch so that the Switches can be interconnected.
2. Check information about the IS-IS interface on each Switch with the default priority.
3. Configure the DIS priority on the Switch.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in **Figure 3-18**
- IP address of each VLANIF interface, as shown in **Figure 3-18**
- System ID, level, and area ID of each Switch
  - SwitchA: The system ID is 0000.0000.0001; the area ID is 10; the DIS priority is 100; the level is Level-1.
  - SwitchB: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-1-2.
  - SwitchC: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-1.
  - SwitchD: The system ID is 0000.0000.0004; the area ID is 10; the level is Level-2.

Configuration Procedure

1. Configure the IDs of the VLANs to which the interfaces belong.

   The configuration details are not mentioned here.
2. Assign IP addresses to VLANIF interfaces.

   The configuration details are not mentioned here.
3. Display the MAC address of the VLANIF 10 interface on each Switch.

   # Display the MAC address of the VLANIF 10 interface on SwitchA.

```
[SwitchA] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                  VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.1        0200-0000-dc00            I -           Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

   # Display the MAC address of the VLANIF 10 interface on SwitchB.

```
[SwitchB] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                  VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.2        00e0-fccd-acdf            I -           Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

   # Display the MAC address of the VLANIF 10 interface on SwitchC.

```
[SwitchC] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                  VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.3        00e0-1396-1600            I -           Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

   # Display the MAC address of the VLANIF 10 interface on SwitchD.

```
[SwitchD] display arp interface vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE          INTERFACE   VPN-INSTANCE
                                                  VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.4        00e0-fcfd-305c            I -           Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0    Interface:1
```

4. Configure basic IS-IS functions.

   # Configure SwitchA.

```
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis enable 1
[SwitchA-Vlanif10] quit
```

Configure SwitchB.

```
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] isis enable 1
[SwitchB-Vlanif10] quit
```

Configure SwitchC.

```
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] is-level level-1
[SwitchC-isis-1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] isis enable 1
[SwitchC-Vlanif10] quit
```

Configure SwitchD.

```
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 10.0000.0000.0004.00
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] quit
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] isis enable 1
[SwitchD-Vlanif10] quit
```

Display information about the IS-IS neighbors of SwitchA.

```
[SwitchA] display isis peer

                        Peer information for ISIS(1)
                        ----------------------------
  System Id       Interface     Circuit Id         State HoldTime   Type
PRI
0000.0000.0002    Vlanif10      0000.0000.0002.01  Up    9s         L1
(L1L2)   64
0000.0000.0003    Vlanif10      0000.0000.0002.01  Up    27s        L1
64
0000.0000.0002    Vlanif10      0000.0000.0004.01  Up    28s        L2(L1L2)
64
0000.0000.0004    Vlanif10      0000.0000.0004.01  Up    8s         L2
64
```

Display information about the IS-IS interfaces on SwitchA.

```
[SwitchA] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface       Id      IPV4.State          MTU    Type   DR
 Vlanif10        001         Up              1497   L1/L2  No/No
```

Display information about the IS-IS interfaces on SwitchB.

```
[SwitchB] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface       Id      IPV4.State          MTU    Type   DR
 Vlanif10        001         Up              1497   L1/L2  Yes/No
```

Display information about the IS-IS interfaces on SwitchD.

```
[SwitchD] display isis interface

                    Interface information for ISIS(1)
```

```
                    ---------------------------------
 Interface       Id      IPV4.State          MTU    Type   DR
 Vlanif10        001         Up              1497   L1/L2  No/Yes
```

NOTE

When the default DIS priority is used,

- The MAC address of the interface on SwitchB is the largest one among that of the interfaces on the Level-1 Switchs. Thus, SwitchB is elected as the Level-1 DIS.
- The MAC address of the interface on SwitchD is the largest one among that of the interfaces on the Level-2 Switchs. Thus, SwitchD is elected as the Level-2 DIS.

The Level-1 pseudonode is 0000.0000.0002.01. The Level-2 pseudonode is 0000.0000.0004.01.

5. Configure the DIS priority of SwitchA.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis dis-priority 100
[SwitchA-Vlanif10] quit
```

Display information about the IS-IS neighbors of SwitchA.

```
[SwitchA] display isis peer

                        Peer information for ISIS(1)
                        ----------------------------
  System Id       Interface       Circuit Id          State HoldTime Type
PRI
0000.0000.0002     Vlanif10         0000.0000.0001.01    Up   21s       L1
(L1L2)  64
0000.0000.0003     Vlanif10        0000.0000.0001.01    Up   27s       L1
64
0000.0000.0002     Vlanif10         0000.0000.0001.01    Up   28s       L2
(L1L2)  64
0000.0000.0004     Vlanif10        0000.0000.0001.01    Up   30s       L2
64
```

6. Verify the configuration.

Display information about the IS-IS interfaces on SwitchA.

```
[SwitchA] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface       Id      IPV4.State          MTU   Type   DR
 Vlanif10        001         Up              1497  L1/L2  Yes/Yes
```

As displayed above, after the DIS priority of the IS-IS interface is changed, SwitchA immediately becomes a Level-1-2 DIS and its pseudonode is 0000.0000.0001.01.

Display information about the IS-IS neighbors and IS-IS interfaces on SwitchB.

```
[SwitchB] display isis peer

                        Peer information for ISIS(1)
                        ----------------------------
  System Id       Interface       Circuit Id          State HoldTime   Type
PRI
0000.0000.0001     Vlanif10         0000.0000.0001.01    Up   7s          L1
(L1L2) 100
0000.0000.0003     Vlanif10         0000.0000.0001.01    Up   25s
L1        64
0000.0000.0001     Vlanif10         0000.0000.0001.01    Up   7s          L2
(L1L2) 100
0000.0000.0004     Vlanif10         0000.0000.0001.01    Up   25s
L2        64
[SwitchB] display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface       Id      IPV4.State          MTU   Type   DR
 Vlanif10        001         Up              1497  L1/L2  No/No
```

Display information about the IS-IS neighbors and IS-IS interfaces on SwitchD.

```
[SwitchD] display isis peer

                        Peer information for ISIS(1)
                        ----------------------------
  System Id       Interface       Circuit Id         State HoldTime   Type
PRI
0000.0000.0001    Vlanif10        0000.0000.0001.01    Up   9s         L2
100
0000.0000.0002    Vlanif10         0000.0000.0001.01    Up   28s
L2       64
[SwitchD] display isis interface

                     Interface information for ISIS(1)
                     ---------------------------------
 Interface       Id      IPV4.State          MTU   Type   DR
 Vlanif10        001         Up              1497  L1/L2  No/No
```

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10
#
isis 1
network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 isis dis-priority 100
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 10
#
isis 1
network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 vlan batch 10
#
isis 1
 is-level level-1
network-entity 10.0000.0000.0003.00
#
```

```
interface Vlanif10
 ip address 10.1.1.3 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 vlan batch 10
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0004.00
#
interface Vlanif10
 ip address 10.1.1.4 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

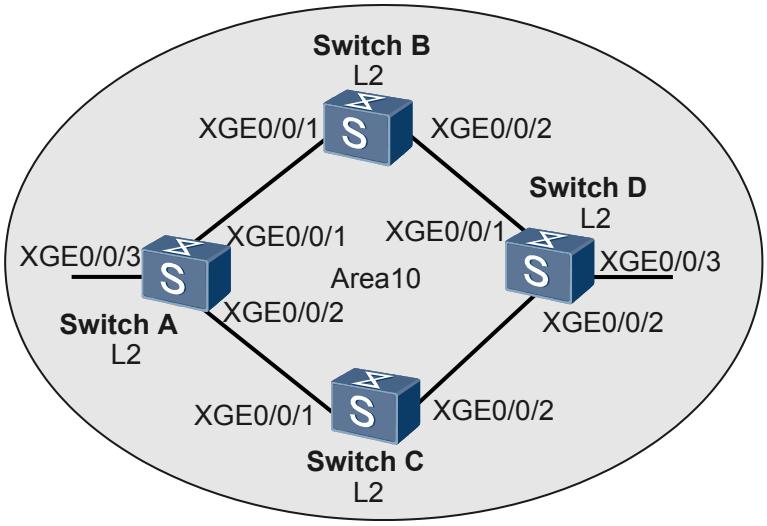
3.6.6 Example for Configuring IS-IS Load Balancing

Networking Requirements

As shown in **Figure 3-19**:

- SwitchA, SwitchB, SwitchC, and SwitchD are interconnected in an IP network by running the IS-IS protocol.
- SwitchA, SwitchB, SwitchC, and SwitchD are Level-2 Switchs in Area 10.
- Load balancing is required for the transmission of the traffic from SwitchA to SwitchD through SwitchB and SwitchC respectively.

Figure 3-19 Networking diagram for configuring IS-IS load balancing



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	10.1.1.1/24
SwitchA	XGE 0/0/2	VLANIF 20	10.1.2.1/24
SwitchA	XGE 0/0/3	VLANIF 50	172.16.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	10.1.1.2/24
SwitchB	XGE 0/0/2	VLANIF 30	192.168.0.1/24
SwitchC	XGE 0/0/1	VLANIF 20	10.1.2.2./24
SwitchC	XGE 0/0/2	VLANIF 40	192.168.1.1/24
SwitchD	XGE 0/0/1	VLANIF 30	192.168.0.2/24
SwitchD	XGE 0/0/2	VLANIF 40	192.168.1.2/24
SwitchD	XGE 0/0/3	VLANIF 60	172.17.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each Switch so that the Switches can be interconnected.
2. Set the number of equal-cost routes to 1 to carry out load balancing, and check information about the routing table.
3. Configure load balancing on SwitchA and check information about the routing table.
4. (Optional) Configure the preference for equal-cost routes on SwitchA.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in **Figure 3-19**

- IP address of each VLANIF interface, as shown in **Figure 3-19**
- System ID, level, and area ID of each Switch
  - Switch A: The system ID is 0000.0000.0001; the area ID is 10; the level is Level-2.
  - Switch B: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-2.
  - Switch C: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-2.
  - Switch D: The system ID is 0000.0000.0004; the area ID is 10; the level is Level-2.
- Number of equal-cost routes for load balancing on Switch A: 1
- Load balancing mode on Switch A
- Weight for the preference of the equal-cost routes on Switch C: 1

Configuration Procedure

1. Configure the IDs of the VLANs to which the interfaces belong.

   The configuration details are not mentioned here.
2. Assign IP addresses to VLANIF interfaces.

   The configuration details are not mentioned here.
3. Configure basic IS-IS functions.

   The configuration details are not mentioned here.
4. Set the number of equal-cost routes for load balancing to 1 on Switch A.

```
[SwitchA] isis 1
[SwitchA-isis-1] maximum load-balancing 1
[SwitchA-isis-1] quit
```

   # Display the routing table of SwitchA.

```
[SwitchA] display isis route

                        Route information for ISIS(1)
                        ------------------------------

                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------

 IPV4 Destination      IntCost   ExtCost   ExitInterface   NextHop
Flags
-------------------------------------------------------------------------------
 192.168.1.0/24        20         NULL     Vlanif20        10.1.2.2
A/-/-/-
 10.1.1.0/24           10         NULL     Vlanif10        Direct          D/-/
L/-
 172.16.1.0/24         10         NULL     Vlanif50        Direct          D/-/
L/-
 172.17.1.0/24         30         NULL     Vlanif10        10.1.1.2
A/-/-/-
 10.1.2.0/24           10         NULL     Vlanif20        Direct          D/-/
L/-
 192.168.0.0/24        20         NULL     Vlanif10        10.1.1.2
A/-/-/-

     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

   As shown in the routing table, when the maximum number of equal-cost routes for load balancing is set to 1, IS-IS chooses the next hop 10.1.1.2 (Switch B) as the only best route to the destination network 172.17.1.0. This is because Switch B has a smaller system ID.
5. Restore the default number of equal-cost routes for load balancing on Switch A.

```
[SwitchA] isis 1
[SwitchA-isis-1] undo maximum load-balancing
```

```
[SwitchA-isis-1] quit
```

Display the routing table of SwitchA.

```
[SwitchA] display isis route

                        Route information for ISIS(1)
                        ------------------------------

                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------

 IPV4 Destination      IntCost   ExtCost   ExitInterface   NextHop
Flags
-------------------------------------------------------------------------------
 192.168.1.0/24        20         NULL     Vlanif20        10.1.2.2
A/-/-/-
 10.1.1.0/24           10         NULL     Vlanif10        Direct           D/-/
L/-
 172.16.1.0/24         10         NULL     Vlanif50        Direct           D/-/
L/-
 172.17.1.0/24         30         NULL     Vlanif10        10.1.1.2
A/-/-/-
                                           Vlanif20        10.1.2.2
 10.1.2.0/24           10         NULL     Vlanif20        Direct           D/-/
L/-
 192.168.0.0/24        20         NULL     Vlanif10        10.1.1.2
A/-/-/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

As shown in the routing table, the number of equal-cost routes for load balancing is restored to the default value of 6. Both the next hops of Switch A, 10.1.1.2 (that is, SwitchB) and 10.1.2.2 (that is, SwitchC) now become valid.

6. (Optional) Configure the preference for equal-cost routes on Switch A.

   If you do not perform load balancing through Switch B and SwitchC, configure the preference of the equal-cost routes and specify the next hop.

```
[SwitchA] isis
[SwitchA-isis-1] nexthop 10.1.2.2 weight 1
[SwitchA-isis-1] quit
```

7. Verify the configuration.

   # Display the routing table of SwitchA.

```
[SwitchA] display isis route
                        Route information for ISIS(1)
                        ------------------------------

                       ISIS(1) Level-2 Forwarding Table
                       --------------------------------

 IPV4 Destination     IntCost    ExtCost   ExitInterface   NextHop
Flags
-------------------------------------------------------------------------------
--
 192.168.1.0/24       20         NULL      Vlanif20        10.1.2.2
A/-/-/-
 10.1.1.0/24          10         NULL      Vlanif10        Direct           D/-/
L/-
 172.16.1.0/24        10         NULL      Vlanif50        Direct           D/-/
L/-
 172.17.1.0/24        30         NULL      Vlanif20        10.1.2.2
A/-/-/-
 10.1.2.0/24          10         NULL      Vlanif20        Direct           D/-/
L/-
 192.168.0.0/24       20         NULL      Vlanif10        10.1.1.2
A/-/-/-
```

```
      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

As shown in the routing table, the preference (with the weight of 1) of the next hop 10.1.2.2, the Switch C, is higher than that of 10.1.1.2, the Switch B, after the preference is configured for equal-cost routes. Thus, IS-IS chooses the next hop 10.1.2.2 as the best route.

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10 20 50
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0001.00
 nexthop 10.1.2.2 weight
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif50
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10 30
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
```

```
 port trunk allow-pass vlan 30
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 20 40
#
isis 1
is-level level-2
 network-entity 10.0000.0000.0003.00
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 vlan batch 30 40 60
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0004.00
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
#
interface Vlanif60
 ip address 172.17.1.1 255.255.255.0
isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 60
#
return
```

3.7 BGP Configuration

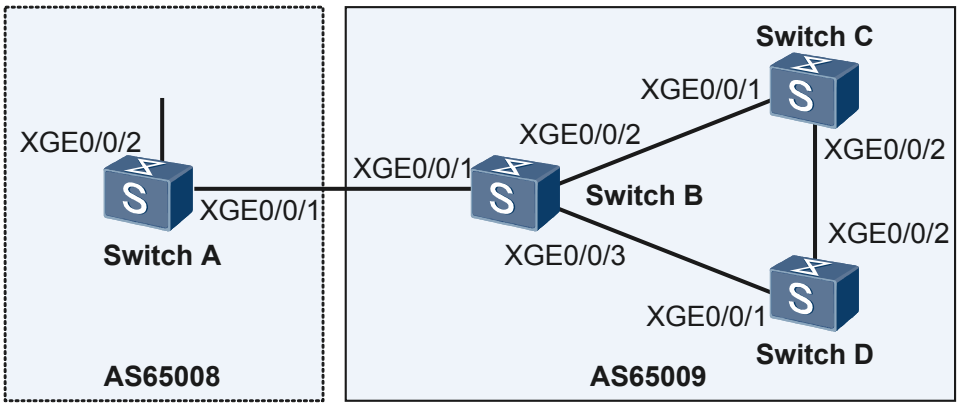
BGP is used between ASs to transmit routing information on large-scale and complex networks.

3.7.1 Example for Configuring Basic BGP Functions

Networking Requirements

As shown in **Figure 3-20**, all Switchs run BGP. An EBGP peer relationship is set up between SwitchA and SwitchB. IBGP peer relationships are set up between SwitchB, SwitchC, and SwitchD.

Figure 3-20 Networking diagram for configuring basic BGP functions



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	200.1.1.2/24
SwitchA	XGE 0/0/2	VLANIF 50	8.1.1.1/8
SwitchB	XGE 0/0/1	VLANIF 10	200.1.1.1/24
SwitchB	XGE 0/0/2	VLANIF 20	9.1.3.1/24
SwitchB	XGE 0/0/3	VLANIF 30	9.1.1.1/24
SwitchC	XGE 0/0/1	VLANIF 20	9.1.3.2/24
SwitchC	XGE 0/0/2	VLANIF 40	9.1.2.1/24
SwitchD	XGE 0/0/1	VLANIF 30	9.1.1.2/24
SwitchD	XGE 0/0/2	VLANIF 40	9.1.2.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Set up IBGP peer relationships between SwitchB, SwitchC and SwitchD.
2. Create an EBGP peer relationship between SwitchA and SwitchB.

3. Advertise routes through the **network** command on SwitchA and check the routing tables of SwitchA, SwitchB, and SwitchC.
4. Configure BGP on SwitchB to import direct routes, and check the routing tables of SwitchA and SwitchC.

Data Preparation

To complete the configuration, you need the following data:

- The VLAN ID of each interface is shown in **Figure 3-20**.
- The IP address of each VLANIF interface is shown in **Figure 3-20**.
- The router ID of SwitchA is 1.1.1.1 and the number of the AS where it resides is 65008.
- The router IDs of SwitchB, SwitchC, and SwitchD are 2.2.2.2, 3.3.3.3. and 4.4.4.4, and the number of the AS where they reside is 65009.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.
2. Assign an IP address to each VLANIF interface.

   The configuration details are not mentioned here.
3. Create IBGP peer relationships.

   # Configure SwitchB.

```
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] peer 9.1.3.2 as-number 65009
```

   # Configure SwitchC.

```
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 9.1.3.1 as-number 65009
[SwitchC-bgp] peer 9.1.2.2 as-number 65009
[SwitchC-bgp] quit
```

   Configure SwitchD

```
[SwitchD] bgp 65009
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] peer 9.1.1.1 as-number 65009
[SwitchD-bgp] peer 9.1.2.1 as-number 65009
[SwitchD-bgp] quit
```

4. Create an EBGP peer relationship.

   # Configure SwitchA

```
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
```

   # Configure SwitchB.

```
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] quit
```

   # Check the status of BGP connections.

```
[SwitchB] display bgp peer

 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 3                 Peers in established state : 3
```

```
  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  9.1.1.2         4 65009       49       62     0 00:44:58 Established       0
  9.1.3.2         4 65009       56       56     0 00:40:54 Established       0
  200.1.1.2       4 65008       49       65     0 00:44:03 Established       1
```

You can view that the BGP connections between SwitchB and all the other S-switchs are set up.

5. Configure SwitchA to advertise the route 8.0.0.0/8.

   Configure SwitchA to advertise routes.

```
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-af-ipv4] network 8.0.0.0 255.0.0.0
[SwitchA-bgp-af-ipv4] quit
[SwitchA-bgp] quit
```

   # Check the routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.0.0.0         0.0.0.0         0                      0      i
```

   # Check the routing table of SwitchB.

```
[SwitchB] display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.0.0.0         200.1.1.2       0                      0      65008i
```

   # Check the routing table of SwitchC.

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 1

 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

   i  8.0.0.0         200.1.1.2       0          100        0      65008i
```

   From the routing table, you can view that SwitchC has learned the route to the destination 8.0.0.0 in AS 65008, but the next hop 200.1.1.2 is unreachable. Therefore, this route is invalid.

6. Configure BGP to import direct routes

   # Configure SwitchB.

```
[SwitchB] vlan 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] import-route direct
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

   # Check the BGP routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 4

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.0.0.0          0.0.0.0         0                     0      i
 *>   9.1.1.0/24         200.1.1.1       0                     0      65009?
 *>   9.1.3.0/24         200.1.1.1       0                     0      65009?
 *    200.1.1.0       200.1.1.1       0                     0      65009?
```

Check the BGP routing table of SwitchC.

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 4
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 * i  8.0.0.0          200.1.1.2       0          100        0      65008i
 *>i  9.1.1.0/24         9.1.3.1         0          100        0      ?
   i  9.1.3.0/24         9.1.3.1         0          100        0      ?
 *>i  200.1.1.0       9.1.3.1         0          100        0      ?
```

You can view that the route to 8.0.0.0 becomes valid, and the next hop is the address of SwitchA.

Perform the ping operation to verify the configuration.

```
[SwitchC] ping 8.1.1.1
  PING 8.1.1.1: data bytes, press CTRL_C to break
    Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=254 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=254 time=47 ms
    Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=254 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=254 time=16 ms
    Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=254 time=31 ms

  --- 8.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 16/31/47 ms
```

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10 50
#
interface Vlanif10
 ip address 200.1.1.2 255.255.255.0
#
interface Vlanif50
 ip address 8.1.1.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 50
#
```

```
bgp 65008
 router-id 1.1.1.1
 peer 200.1.1.1 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  network 8.0.0.0
  peer 200.1.1.1 enable
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 10 20 30
#
interface Vlanif10
 ip address 200.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 9.1.3.1 255.255.255.0
#
interface Vlanif30
 ip address 9.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65009
 router-id 2.2.2.2
 peer 9.1.1.2 as-number 65009
 peer 9.1.3.2 as-number 65009
 peer 200.1.1.2 as-number 65008
#
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 9.1.1.2 enable
  peer 9.1.3.2 enable
  peer 200.1.1.2 enable
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 9.1.3.2 255.255.255.0
#
interface Vlanif40
 ip address 9.1.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
```

```
 port link-type trunk
 port trunk allow-pass vlan 40
#
bgp 65009
 router-id 3.3.3.3
 peer 9.1.3.1 as-number 65009
 peer 9.1.2.2 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  peer 9.1.3.1 enable
  peer 9.1.2.2 enable
#
return
```

- Configuration file of SwitchD

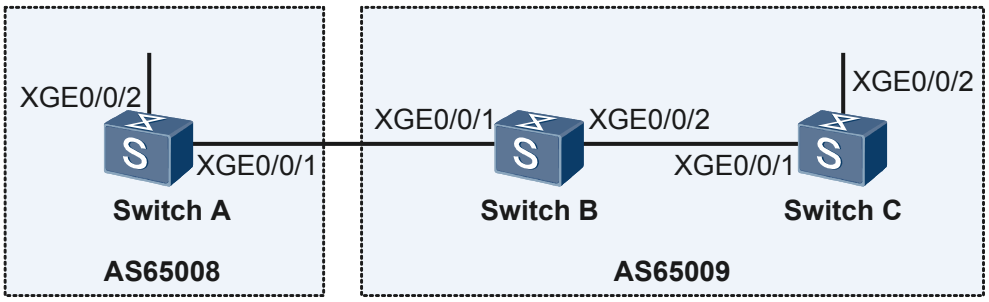
```
#
 sysname SwitchD
#
 vlan batch 30 40
#
interface Vlanif30
 ip address 9.1.1.2 255.255.255.0
#
interface Vlanif40
 ip address 9.1.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
bgp 65009
 router-id 4.4.4.4
 peer 9.1.1.1 as-number 65009
 peer 9.1.2.1 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  peer 9.1.1.1 enable
  peer 9.1.2.1 enable
#
return
```

3.7.2 Example for Configuring BGP to Interact with an IGP

Networking Requirements

As shown in **Figure 3-21**, OSPF is used inside AS 65009. An EBGP peer relationship is set up between SwitchA and SwitchB. SwitchC runs OSPF instead of BGP.

Figure 3-21 Networking diagram for configuring BGP to interact with an IGP



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	3.1.1.2/24
SwitchA	XGE 0/0/2	VLANIF 30	8.1.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	3.1.1.1/24
SwitchB	XGE 0/0/2	VLANIF 20	9.1.1.1/24
SwitchC	XGE 0/0/1	VLANIF 20	9.1.1.2/24
SwitchC	XGE 0/0/2	VLANIF 40	9.1.2.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on SwitchB and SwitchC.
2. Create an EBGP peer relationship on SwitchA and SwitchB.
3. Configure BGP to interact with OSPF on SwitchB and check the routes.
4. Configure BGP route aggregation on SwitchB to simplify the BGP routing table.

Data Preparation

To complete the configuration, you need the following data:

- The VLAN ID of each interface is shown in **Figure 3-21**.
- The IP address of each VLANIF interface is shown in **Figure 3-21**.
- The router ID of SwitchA is 1.1.1.1 and the number of the AS where it resides is 65008.
- The router IDs of SwitchB and SwitchC are 2.2.2.2 and 3.3.3.3, and the number of the AS where they reside is 65009.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.
2. Assign an IP address to each VLANIF interface.

   The configuration details are not mentioned here.
3. Configure OSPF.

Configure SwitchB.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure SwitchC.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

4. Create an EBGP peer relationship.

   Configure SwitchA.

```
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 3.1.1.1 as-number 65009
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-af-ipv4] network 8.1.1.0 255.255.255.0
[SwitchA-bgp-af-ipv4] quit
[SwitchA-bgp] quit
```

   # Configure SwitchB.

```
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 3.1.1.2 as-number 65008
```

5. Configure BGP to interact with an IGP

   # On SwitchB, configure BGP to import OSPF routes.

```
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] import-route ospf 1
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

   # Check the routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 3

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>   8.1.1.0/24         0.0.0.0         0                      0      i
 *>   9.1.1.0/24         3.1.1.1         0                      0      65009?
 *>   9.1.2.0/24         3.1.1.1         2                      0      65009?
```

   # On SwitchB, configure BGP to import BGP routes.

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

   # Check the routing table of SwitchC.

```
[SwitchC] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost      Flags    NextHop        Interface

        8.1.1.0/24  O_ASE   150  1          D         9.1.1.1       Vlanif20
        9.1.1.0/24  Direct  0    0          D         9.1.1.2       Vlanif20
```

```
      9.1.1.2/32  Direct  0    0         D         127.0.0.1     InLoopBack0
      9.1.2.0/24  Direct  0    0         D         9.1.2.1       Vlanif40
      9.1.2.1/32  Direct  0    0         D         127.0.0.1     InLoopBack0
    127.0.0.0/8   Direct  0    0         D         127.0.0.1     InLoopBack0
    127.0.0.1/32  Direct  0    0         D         127.0.0.1     InLoopBack0
```

6. Configure automatic aggregation.

   # Configure SwitchB.

```
[SwitchB] bgp 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] summary automatic
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

   # Check the BGP routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   8.1.1.0/24         0.0.0.0         0                      0      i
 *>   9.0.0.0            3.1.1.1                                0      65009?
```

   # Perform the ping operation to verify the configuration.

```
[SwitchA] ping -a 8.1.1.1 9.1.2.1
  PING 9.1.2.1: 56  data bytes, press CTRL_C to break
    Reply from 9.1.2.1: bytes=56 Sequence=1 ttl=254 time=15 ms
    Reply from 9.1.2.1: bytes=56 Sequence=2 ttl=254 time=31 ms
    Reply from 9.1.2.1: bytes=56 Sequence=3 ttl=254 time=47 ms
    Reply from 9.1.2.1: bytes=56 Sequence=4 ttl=254 time=46 ms
    Reply from 9.1.2.1: bytes=56 Sequence=5 ttl=254 time=47 ms
  --- 9.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 15/37/47 ms
```

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 3.1.1.2 255.255.255.0
#
interface Vlanif30
 ip address 8.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65008
 router-id 1.1.1.1
 peer 3.1.1.1 as-number 65009
 #
```

```
 ipv4-family unicast
  undo synchronization
  network 8.1.1.0 255.255.255.0
  peer 3.1.1.1 enable
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 3.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 9.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
bgp 65009
 router-id 2.2.2.2
 peer 3.1.1.2 as-number 65008
 #
 ipv4-family unicast
  undo synchronization
  summary automatic
  import-route ospf 1
  peer 3.1.1.2 enable
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 9.1.1.0 0.0.0.255
return
```

- Configuration file of SwitchC

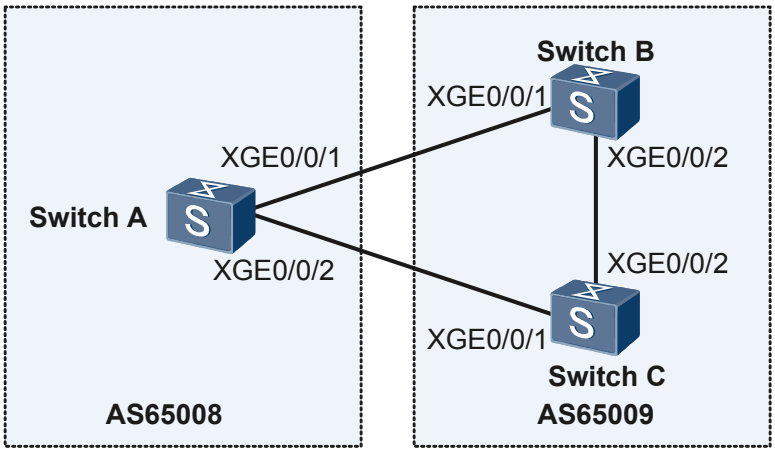
```
#
 sysname SwitchC
#
 vlan batch 20 40
#
interface Vlanif20
 ip address 9.1.1.2 255.255.255.0
#
interface Vlanif40
 ip address 9.1.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 40
#
ospf 1
 area 0.0.0.0
  network 9.1.1.0 0.0.0.255
  network 9.1.2.0 0.0.0.255
#
return
```

3.7.3 Example for Configuring BGP Load Balancing and the MED

Networking Requirements

As shown in **Figure 3-22**, all Switchs run BGP. SwitchA resides in AS 65008. Both SwitchB and SwitchC reside in AS 65009. EBGP runs among SwitchA, SwitchB, and SwitchC. IBGP runs between SwitchB and SwitchC.

Figure 3-22 Networking diagram of BGP route selection



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	200.1.1.2/24
SwitchA	XGE 0/0/2	VLANIF 20	200.1.2.2/24
SwitchB	XGE 0/0/1	VLANIF 10	200.1.1.1/24
SwitchB	XGE 0/0/2	VLANIF 30	9.1.1.1/24
SwitchC	XGE 0/0/1	VLANIF 20	200.1.2.1/24
SwitchC	XGE 0/0/2	VLANIF 30	9.1.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Set up EBGP peer relationships between SwitchA and SwitchB, and between SwitchA and SwitchC. Create an IBGP peer relationship between SwitchB and SwitchC.
2. Configure load balancing and the MED on SwitchA and check the routing table.

Data Preparation

To complete the configuration, you need the following data:

- The VLAN ID of each interface is shown in **Figure 3-22**.
- The IP address of each VLANIF interface is shown in **Figure 3-22**.

- The router IDs of SwitchA is 1.1.1.1, the number of the AS where it resides is 65008, and the number of routes for load balancing is 2.
- The router IDs of SwitchB and SwitchC are 2.2.2.2 and 3.3.3.3, the number of the AS where they reside is 65008, the default MED of SwitchB is 100.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.

2. Assign an IP address to each VLANIF interface.

   The configuration details are not mentioned here.

3. Create EBGP peer relationships.

   Configure SwitchA.

```
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
[SwitchA-bgp] peer 200.1.2.1 as-number 65009
[SwitchA-bgp] quit
```

   # Configure SwitchB.

```
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[SwitchB-bgp-af-ipv4] quit
[SwitchB-bgp] quit
```

   # Configure SwitchC.

```
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 200.1.2.2 as-number 65008
[SwitchC-bgp] peer 9.1.1.1 as-number 65009
[SwitchC-bgp] ipv4-family unicast
[SwitchC-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[SwitchC-bgp-af-ipv4] quit
[SwitchC-bgp] quit
```

   # Check the routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24        200.1.1.1       0                     0       65009i
 *                      200.1.2.1       0                     0       65009i
```

   You can view that there are two valid routes to the destination 9.1.1.0/24. The route whose next hop is 200.1.1.1 is the optimal route because the router ID of SwitchB is smaller.

4. Configure load balancing.

   Configure SwitchA.

```
[SwitchA] bgp 65008
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-af-ipv4] maximum load-balancing 2
[SwitchA-bgp-af-ipv4] quit
```

```
[SwitchA-bgp] quit
```

Check the routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         200.1.1.1       0                    0      65009i
 *>                      200.1.2.1       0                    0      65009i
```

You can view that the BGP route 9.1.1.0/24 has two next hops that are 200.1.1.1 and 200.1.2.1. Both of them are optimal routes.

5. Set the MED.

   # Set the MED sent by SwitchB to SwitchA through the policy.

```
[SwitchB] route-policy 10 permit node 10
[SwitchB-route-policy] apply cost 100
[SwitchB-route-policy] quit
[SwitchB] bgp 65009
[SwitchB-bgp] peer 200.1.1.2 route-policy 10 export
```

   # Check the routing table of SwitchA.

```
[SwitchA] display bgp routing-table

 Total Number of Routes: 2

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   9.1.1.0/24         200.1.2.1       0                    0      65009i
 *                       200.1.1.1       100                  0      65009i
```

   You can view that the MED of route with the next hop as 200.1.1.1 (SwitchB) is 100, and the MED of the route with the next hop as 200.1.2.1 is 0. Therefore, the route with the smaller MED is selected.

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 200.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 200.1.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
bgp 65008
```

```
 router-id 1.1.1.1
 peer 200.1.1.1 as-number 65009
 peer 200.1.2.1 as-number 65009
 #
 ipv4-famlily unicast
  undo synchronization
  maximum load-balancing 2
  peer 200.1.1.1 enable
  peer 200.1.2.1 enable
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 10 30
#
interface Vlanif10
 ip address 200.1.1.1 255.255.255.0
#
interface Vlanif30
 ip address 9.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65009
 router-id 2.2.2.2
 peer 200.1.1.2 as-number 65008
 peer 9.1.1.2 as-number 65009
 #
 ipv4-family unicast
  undo synchronization
  network 9.1.1.0 255.255.255.0
  peer 200.1.1.2 enable
  peer 200.1.1.2 route-policy 10 export
  peer 9.1.1.2 enable
#
route-policy 10 permit node 10
 apply cost 100
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 vlan batch 20 30
#
interface Vlanif10
 ip address 200.1.2.1 255.255.255.0
#
interface Vlanif30
 ip address 9.1.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
bgp 65009
```

```
 router-id 3.3.3.3
 peer 9.1.1.1 as-number 65009
 peer 200.1.2.2 as-number 65008
 #
 ipv4-family unicast
  undo synchronization
  network 9.1.1.0 255.255.255.0
  peer 9.1.1.1 enable
  peer 200.1.2.2 enable
#
return
```

3.8 MBGP Configuration

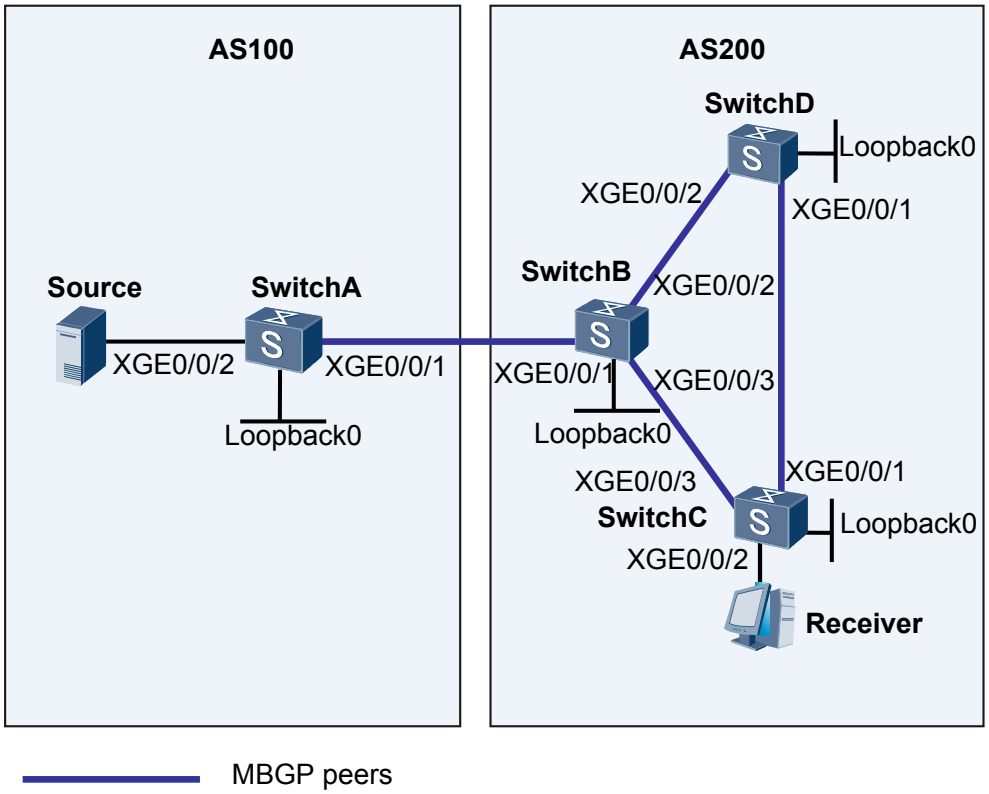
MBGP is dedicated to transmitting multicast routing information across ASs.

3.8.1 Example for Configuring Basic MBGP Functions

Networking Requirements

As shown in **Figure 3-23**, the receiver receives VOD information in multicast mode. The receiver and the source reside in different ASs. The MBGP peer relationship is established between ASs to transmit multicast routing information.

Figure 3-23 Networking diagram of MBGP configuration



Switch	Interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF100	192.1.1.1/24
	XGE 0/0/2	VLANIF101	10.10.10.1/24

	Loopback0		1.1.1.1/32
Switch B	XGE 0/0/1	VLANIF100	192.1.1.2/24
	XGE 0/0/2	VLANIF200	194.1.1.2/24
	XGE 0/0/3	VLANIF300	193.1.1.2/24
	Loopback0		2.2.2.2/32
Switch C	XGE 0/0/1	VLANIF400	195.1.1.1/24
	XGE 0/0/2	VLANIF102	22.22.22.1/24
	XGE 0/0/3	VLANIF300	193.1.1.1/24
	Loopback0		3.3.3.3/32
Switch D	XGE 0/0/1	VLANIF400	195.1.1.2/24
	XGE 0/0/2	VLANIF200	194.1.1.1/24
	Loopback0		4.4.4.4/32

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP addresses for the interfaces on each Switch to ensure internetworking within the AS in unicast mode.
2. Configure the MBGP peer and set up inter-AS multicast routes.
3. Configure the MBGP routes to be advertised.
4. Enable multicast on each Switch.
5. Configure basic PIM-SM functions in each AS and enable the IGMP function on the interfaces at the host side.
6. Configure the BSR boundary on the interfaces connecting two ASs.
7. Configure the MSDP peers to transfer inter-AS multicast information.

Data Preparation

To complete the configuration, you need the following data:

- AS number of Switch A: 100
- AS number of Switch B, Switch C, and Switch D: 200
- Address of the multicast group (225.1.1.1) and address of the multicast source (10.10.10.10/24)

NOTE

This configuration example describes only the commands used to configure MBGP.

Procedure

Step 1 Configure the IP addresses for the interfaces on each Switch and the OSPF protocol in the ASs.

Configure the IP addresses and masks of the interfaces on each Switch according to **Figure 3-23**. Connect the switches through OSPF and ensure that Switch B, Switch C, and Switch D can communicate with each other through the network layer and can learn the routes on the loopback interfaces of each other. Configure the switches to dynamically update routes through

a unicast routing protocol. OSPF process 1 is adopted in the configuration and the procedure is not mentioned here.

Step 2 Configure BGP, enable the MBGP protocol, and configure the MBGP peers.

Configure BGP and the MBGP peer on Switch A.

```
[SwitchA] bgp 100
[SwitchA-bgp] peer 192.1.1.2 as-number 200
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-multicast] peer 192.1.1.2 enable
[SwitchA-bgp-af-multicast] quit
[SwitchA-bgp] quit
```

Configure BGP and the MBGP peer on Switch B.

```
[SwitchB] bgp 200
[SwitchB-bgp] peer 192.1.1.1 as-number 100
[SwitchB-bgp] peer 193.1.1.1 as-number 200
[SwitchB-bgp] peer 194.1.1.1 as-number 200
[SwitchB-bgp] ipv4-family multicast
[SwitchB-bgp-af-multicast] peer 192.1.1.1 enable
[SwitchB-bgp-af-multicast] peer 193.1.1.1 enable
[SwitchB-bgp-af-multicast] peer 194.1.1.1 enable
[SwitchB-bgp-af-multicast] quit
[SwitchB-bgp] quit
```

Configure BGP and the MBGP peer on Switch C.

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.2 as-number 200
[SwitchC-bgp] peer 195.1.1.2 as-number 200
[SwitchC-bgp] ipv4-family multicast
[SwitchC-bgp-af-multicast] peer 193.1.1.2 enable
[SwitchC-bgp-af-multicast] peer 195.1.1.2 enable
[SwitchC-bgp-af-multicast] quit
[SwitchC-bgp] quit
```

Configure BGP and the MBGP peer on Switch D.

```
[SwitchD] bgp 200
[SwitchD-bgp] peer 194.1.1.2 as-number 200
[SwitchD-bgp] peer 195.1.1.1 as-number 200
[SwitchD-bgp] ipv4-family multicast
[SwitchD-bgp-af-multicast] peer 194.1.1.2 enable
[SwitchD-bgp-af-multicast] peer 195.1.1.1 enable
[SwitchD-bgp-af-multicast] quit
[SwitchD-bgp] quit
```

Step 3 Configure the routes to be advertised.

Configure the routes to be advertised on Switch A.

```
[SwitchA] bgp 100
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-multicast] import-route direct
[SwitchA-bgp-af-multicast] quit
[SwitchA-bgp] quit
```

Configure the routes to be advertised on Switch B.

```
[SwitchB] bgp 200
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] ipv4-family multicast
[SwitchB-bgp-af-multicast] import-route direct
[SwitchB-bgp-af-multicast] import-route ospf 1
[SwitchB-bgp-af-multicast] quit
[SwitchB-bgp] quit
```

Configure the routes to be advertised on Switch C. The configuration of Switch D is similar to the configuration of Switch C, and is not mentioned here.

```
[SwitchC] bgp 200
[SwitchC-bgp] ipv4-family multicast
[SwitchC-bgp-af-multicast] import-route direct
[SwitchC-bgp-af-multicast] import-route ospf 1
[SwitchC-bgp-af-multicast] quit
[SwitchC-bgp] quit
```

Step 4 Enable multicast on each Switch and the interfaces that are connected.

Configure Switch A.

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] pim sm
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim sm
[SwitchA-Vlanif101] quit
```

Configure Switch B.

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] pim sm
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] pim sm
[SwitchB-Vlanif200] quit
[SwitchB] interface vlanif 300
[SwitchB-Vlanif300] pim sm
[SwitchB-Vlanif300] quit
```

Configure Switch C.

```
[SwitchC] multicast routing-enable
[SwitchC] interface vlanif 400
[SwitchC-Vlanif400] pim sm
[SwitchC-Vlanif400] quit
[SwitchC] interface vlanif 102
[SwitchC-Vlanif102] pim sm
[SwitchC-Vlanif102] igmp enable
[SwitchC-Vlanif102] quit
[SwitchC] interface vlanif 300
[SwitchC-Vlanif300] pim sm
[SwitchC-Vlanif300] quit
```

Configure Switch D.

```
[SwitchD] multicast routing-enable
[SwitchD] interface vlanif 400
[SwitchD-Vlanif400] pim sm
[SwitchD-Vlanif400] quit
[SwitchD] interface vlanif 200
[SwitchD-Vlanif200] pim sm
[SwitchD-Vlanif200] quit
```

Step 5 Configure BSR and RP within each AS.

Configure Switch A.

```
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 255.255.255.255
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit
[SwitchA] pim
[SwitchA-pim] c-bsr loopback 0
```

```
[SwitchA-pim] c-rp loopback 0
[SwitchA-pim] quit
```

Configure Switch B.

```
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] ip address 2.2.2.2 255.255.255.255
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB] quit
```

Step 6 Configure the BSR boundary on the interfaces connecting two ASs.

Configure Switch A.

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] pim bsr-boundary
[SwitchA-Vlanif100] quit
```

Configure Switch B.

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] pim bsr-boundary
[SwitchB-Vlanif100] quit
```

Step 7 Configure MSDP peers.

Configure Switch A.

```
[SwitchA] msdp
[SwitchA-msdp] peer 192.1.1.2 connect-interface vlanif100
[SwitchA-msdp] quit
```

Configure Switch B.

```
[SwitchB] msdp
[SwitchB-msdp] peer 192.1.1.1 connect-interface vlanif100
[SwitchB-msdp] quit
```

Step 8 Verify the configuration.

Run the **display bgp multicast peer** command to view the MBGP peer relationship between switches. For example, the following information shows the MBGP peer relationship on Switch A:

```
[SwitchA] display bgp multicast peer
BGP local router ID : 1.1.1.1
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1
  Peer        V   AS   MsgRcvd  MsgSent  OutQ  Up/Down   State         PrefRcv
  192.1.1.2   4   200  82       75       0     00:30:29  Established    17
```

Run the **display msdp brief** command to view information about the MSDP peer relationship between switches. For example, the following information shows the MBGP peer relationship on Switch B:

```
[SwitchB] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured      Up        Listen       Connect      Shutdown     Down
  1                 1          0            0            0            0

  Peer's Address       State     Up/Down time    AS     SA Count    Reset Count
  192.1.1.1            Up        00:07:17        100     1            0
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
 vlan batch 100 101
#
 multicast routing-enable
#
interface vlanif 100
 ip address 192.1.1.1 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface vlanif 101
 ip address 10.10.10.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 101
#
interface loopback 0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
pim
 c-bsr loopback 0
 c-rp loopback 0
#
bgp 100
 peer 192.1.1.2 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 192.1.1.2 enable
#
 ipv4-family multicast
  undo synchronization
  import-route direct
  peer 192.1.1.2 enable
#
msdp
 peer 192.1.1.2 connect-interface vlanif100
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 100 200 300
#
 multicast routing-enable
#
interface vlanif 100
 ip address 192.1.1.2 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface vlanif 200
 ip address 194.1.1.2 255.255.255.0
 pim sm
#
interface vlanif 300
 ip address 193.1.1.2 255.255.255.0
```

```
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 200
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 300
#
interface loopback 0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
pim
 c-bsr loopback 0
 c-rp loopback 0
#
ospf 1
 area 0.0.0.0
  network 193.1.1.0 0.0.0.255
  network 194.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
bgp 200
 peer 192.1.1.1 as-number 100
 peer 193.1.1.1 as-number 200
 peer 194.1.1.1 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 192.1.1.1 enable
  peer 193.1.1.1 enable
  peer 194.1.1.1 enable
#
 ipv4-family multicast
  undo synchronization
  import-route direct
  import-route ospf 1
  peer 192.1.1.1 enable
  peer 193.1.1.1 enable
  peer 194.1.1.1 enable
#
msdp
 peer 192.1.1.1 connect-interface vlanif100
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 102 300 400
#
 multicast routing-enable
#
interface vlanif 102
 ip address 22.22.22.1 255.255.255.0
 pim sm
 igmp enable
#
interface vlanif 300
 ip address 193.1.1.1 255.255.255.0
 pim sm
#
interface vlanif 400
 ip address 195.1.1.1 255.255.255.0
 pim sm
#
```

```
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 400
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 102
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 300
#
interface loopback 0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
pim
 c-bsr loopback 0
 c-rp loopback 0
#
ospf 1
 area 0.0.0.0
  network 193.1.1.0 0.0.0.255
  network 195.1.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
bgp 200
 peer 193.1.1.2 as-number 100
 peer 195.1.1.2 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 193.1.1.2 enable
  peer 195.1.1.2 enable
#
 ipv4-family multicast
  undo synchronization
  import-route direct
  import-route ospf 1
  peer 193.1.1.2 enable
  peer 195.1.1.2 enable
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
 vlan batch 200 400
#
 multicast routing-enable
#
interface vlanif 200
 ip address 194.1.1.1 255.255.255.0
 pim sm
#
interface vlanif 400
 ip address 195.1.1.2 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 400
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 200
#
interface loopback 0
 ip address 4.4.4.4 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 194.1.1.0 0.0.0.255
```

```
  network 195.1.1.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
#
bgp 200
 peer 194.1.1.2 as-number 200
 peer 195.1.1.1 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 194.1.1.2 enable
  peer 195.1.1.1 enable
#
 ipv4-family multicast
  undo synchronization
  import-route direct
  import-route ospf 1
  peer 194.1.1.2 enable
  peer 195.1.1.1 enable
#
return
```

3.9 Routing Policy Configuration

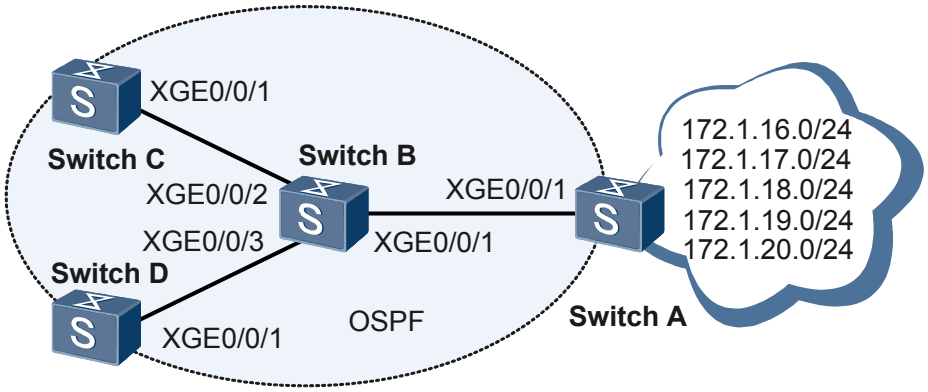
Routing policies are used to filter routes to change the path through which network traffic passes.

3.9.1 Example for Filtering Received and Advertised Routes

Networking Requirements

As shown in **Figure 3-24**, in a network that runs OSPF, Switch-A receives routes from the Internet and provides some of these routes for Switch-B. Switch-A is required to provide 172.1.17.0/24, 172.1.18.0/24, and 172.1.19.0/24 to Switch-B. Switch-C receives only 172.1.18.0/24 and Switch-D receives all routes provided by Switch-B.

Figure 3-24 Networking diagram for filtering received and advertised routes



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	192.168.1.2/24
SwitchB	XGE 0/0/2	VLANIF 20	192.168.2.1/24
SwitchB	XGE 0/0/3	VLANIF 30	192.168.3.1/24

SwitchC	XGE 0/0/1	VLANIF 20	192.168.2.2/24
SwitchD	XGE 0/0/1	VLANIF 30	192.168.3.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of the VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure basic OSPF functions on Switch-A, Switch-B, Switch-C, and Switch-D.
4. Configure static routes on Switch-A and import these routes into OSPF.
5. Configure the policy for advertising routes on Switch-A and check the filtering result on Switch-B.
6. Configure the policy for receiving routes on Switch-C and check the filtering result on Switch-C.

Data Preparation

To complete the configuration, you need the following data:

- Five static routes imported by Switch-A
- Switch-A, Switch-B, Switch-C, and Switch-D located in Area 0, that is, the backbone area
- Names of the IP prefix list and route to be filtered

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.
2. Assign an IP address to each VLANIF interface.

   The configuration details are not mentioned here.
3. Configure basic OSPF functions.

   # Configure Switch-A.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # Configure Switch-B.

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

   # Configure Switch-C.

```
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
```

```
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure Switch-D.

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

4. Configure five static routes on Switch-A and import these routes to OSPF.

```
[SwitchA] ip route-static 172.1.16.0 24 NULL 0
[SwitchA] ip route-static 172.1.17.0 24 NULL 0
[SwitchA] ip route-static 172.1.18.0 24 NULL 0
[SwitchA] ip route-static 172.1.19.0 24 NULL 0
[SwitchA] ip route-static 172.1.20.0 24 NULL 0
[SwitchA] ospf
[SwitchA-ospf-1] import-route static
[SwitchA-ospf-1] quit
```

Check the IP routing table on Switch-B. You view that the five static routes are imported to OSPF.

```
[SwitchB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13       Routes : 13

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D  192.168.1.2     Vlanif10
    192.168.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.2.0/24  Direct 0    0           D  192.168.2.1     Vlanif30
    192.168.2.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.3.0/24  Direct 0    0           D  192.168.3.1     Vlanif20
    192.168.3.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
     172.1.16.0/24  O_ASE  150  1           D  192.168.1.1     Vlanif10
     172.1.17.0/24  O_ASE  150  1           D  192.168.1.1     Vlanif10
     172.1.18.0/24  O_ASE  150  1           D  192.168.1.1     Vlanif10
     172.1.19.0/24  O_ASE  150  1           D  192.168.1.1     Vlanif10
     172.1.20.0/24  O_ASE  150  1           D  192.168.1.1     Vlanif10
```

5. Configure the policy for advertising routes.

Set an IP prefix list named a2b on Switch-A.

```
[SwitchA] ip ip-prefix a2b index 10 permit 172.1.17.0 24
[SwitchA] ip ip-prefix a2b index 20 permit 172.1.18.0 24
[SwitchA] ip ip-prefix a2b index 30 permit 172.1.19.0 24
```

Set a policy for advertising routes on Switch-A and use a2b to filter routes.

```
[SwitchA] ospf
[SwitchA-ospf-1] filter-policy ip-prefix a2b export static
```

Check the routing table on Switch-B. You can view that Switch-B receives only three routes defined in a2b.

```
[SwitchB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11       Routes : 11

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8    Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.1.0/24   Direct 0    0           D  192.168.1.2     Vlanif10
    192.168.1.2/32   Direct 0    0           D  127.0.0.1       InLoopBack0
```

```
    192.168.2.0/24   Direct 0    0           D  192.168.2.1     Vlanif30
    192.168.2.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.3.0/24   Direct 0    0           D  192.168.3.1     Vlanif20
    192.168.3.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
     172.1.17.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
     172.1.18.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
     172.1.19.0/24   O_ASE  150  1           D  192.168.1.1     Vlanif10
```

6. Configure the policy for receiving routes.

   # Set an IP prefix list named in on Switch-C.

   ```
   [SwitchC] ip ip-prefix in index 10 permit 172.1.18.0 24
   ```

   # Set a policy for receiving routes on Switch-C and use in to filter routes.

   ```
   [SwitchC] ospf
   [SwitchC-ospf-1] filter-policy ip-prefix in import
   ```

   # Check the routing table on Switch-C. You can find that Switch-C in the local core routing table receives only one route defined in in.

   ```
   [SwitchC] display ip routing-table
   Route Flags: R - relay, D - download to fib
   ------------------------------------------------------------------------------
   Routing Tables: Public
            Destinations : 6        Routes : 6

   Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

         127.0.0.0/8    Direct 0    0           D  127.0.0.1       InLoopBack0
         127.0.0.1/32   Direct 0    0           D  127.0.0.1       InLoopBack0
       192.168.2.0/24   Direct 0    0           D  192.168.2.2     Vlanif20
       192.168.2.2/32   Direct 0    0           D  127.0.0.1       InLoopBack0
        172.1.18.0/24   O_ASE  150  1           D  192.168.2.1     Vlanif20
   ```

Configuration Files

- Configuration file of Switch-A

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
ospf 1
 filter-policy ip-prefix a2b export static
 import-route static
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
 ip ip-prefix a2b index 10 permit 172.1.17.0 24
 ip ip-prefix a2b index 20 permit 172.1.18.0 24
 ip ip-prefix a2b index 30 permit 172.1.19.0 24
#
 ip route-static 172.1.16.0 255.255.255.0 NULL0
 ip route-static 172.1.17.0 255.255.255.0 NULL0
 ip route-static 172.1.18.0 255.255.255.0 NULL0
 ip route-static 172.1.19.0 255.255.255.0 NULL0
 ip route-static 172.1.20.0 255.255.255.0 NULL0
#
return
```

- Configuration file of Switch-B

```
#
 sysname SwitchB
```

```
#
 vlan batch 10 20 30
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- Configuration file of Switch-C

```
#
 sysname SwitchC
#
 vlan batch 20
#
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
ospf 1
 filter-policy ip-prefix in import
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
 ip ip-prefix in index 10 permit 172.1.18.0 24
#
return
```

- Configuration file of Switch-D

```
#
 sysname SwitchD
#
 vlan batch 30
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
```

```
#
return
```

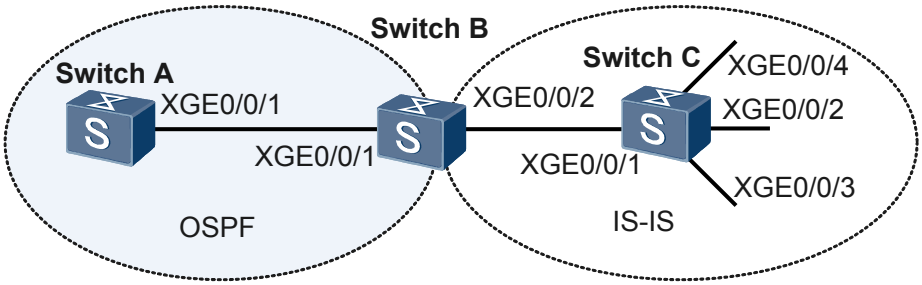
3.9.2 Example for Applying a Routing Policy to Imported Routes

Networking Requirements

As shown in **Figure 3-25**, Switch-B exchanges routing information with Switch-A through OSPF and with Switch-C through IS-IS.

Switch-B is required to import IS-IS routes into OSPF and to use the routing policy to set the route attributes. The cost value of the route 172.17.1.0/24 is set to 100, and the tag of the route 172.17.2.0/24 is set to 20.

Figure 3-25 Networking diagram of applying a routing policy for imported routes



Switch	Interface	VLANIF Interface	IP Address
SwitchA	XGE 0/0/1	VLANIF 10	192.168.1.1/24
SwitchB	XGE 0/0/1	VLANIF 10	192.168.1.2/24
SwitchB	XGE 0/0/2	VLANIF 20	192.168.2.2/24
SwitchC	XGE 0/0/1	VLANIF 20	192.168.2.1/24
SwitchC	XGE 0/0/2	VLANIF 30	172.17.1.1/24
SwitchC	XGE 0/0/3	VLANIF 40	172.17.2.1/24
SwitchC	XGE 0/0/4	VLANIF 50	172.17.3.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of the VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure basic IS-IS functions on Switch-B and Switch-C.
4. Configure OSPF on Switch-A and Switch-B and import IS-IS routes.
5. Configure a routing policy on Switch-B and apply the routing policy when OSPF imports IS-IS routes, and verify the routes.

Data Preparation

To complete the configuration, you need the following data:

- The IS-IS level of Switch-C is Level-2. The system ID is ID 0000.0000.0001. The IS-IS level of Switch-B is Level-2. The system ID is ID 0000.0000.0002. The area number of Switch-B and Switch-C is 10.
- Switch-A and Switch-B are located in Area 0, that is, the backbone area.
- Configure the names of the filtering list and IP prefix list. The cost of the route 172.17.1.0/24 is 100 and the tag of the route 172.17.2.0/24 is 20.

Configuration Procedure

1. Create a VLAN to which each interface belongs.

   The configuration details are not mentioned here.

2. Assign an IP address to each VLANIF interface.

   The configuration details are not mentioned here.

3. Configure IS-IS.

   # Configure Switch-C.

   ```
   [SwitchC] isis
   [SwitchC-isis-1] is-level level-2
   [SwitchC-isis-1] network-entity 10.0000.0000.0001.00
   [SwitchC-isis-1] quit
   [SwitchC] interface vlanif 20
   [SwitchC-Vlanif20] isis enable
   [SwitchC-Vlanif20] quit
   [SwitchC] interface vlanif 30
   [SwitchC-Vlanif30] isis enable
   [SwitchC-Vlanif30] quit
   [SwitchC] interface vlanif 40
   [SwitchC-Vlanif30] isis enable
   [SwitchC-Vlanif30] quit
   [SwitchC] interface vlanif 50
   [SwitchC-Vlanif30] isis enable
   [SwitchC-Vlanif30] quit
   ```

   # Configure Switch-B.

   ```
   [SwitchB] isis
   [SwitchB-isis-1] is-level level-2
   [SwitchB-isis-1] network-entity 10.0000.0000.0002.00
   [SwitchB-isis-1] quit
   [SwitchB] interface vlanif 20
   [SwitchB-Vlanif20] isis enable
   [SwitchB-Vlanif20] quit
   ```

4. Configure OSPF and import routes.

   # Configure Switch-A and enable OSPF.

   ```
   [SwitchA] ospf
   [SwitchA-ospf-1] area 0
   [SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [SwitchA-ospf-1-area-0.0.0.0] quit
   [SwitchA-ospf-1] quit
   ```

   # Configure Switch-B, enable OSPF, and import IS-IS routes.

   ```
   [SwitchB] ospf
   [SwitchB-ospf-1] area 0
   [SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [SwitchB-ospf-1-area-0.0.0.0] quit
   [SwitchB-ospf-1] import-route isis 1
   [SwitchB-ospf-1] quit
   ```

Check the OSPF routing table of Switch-A. You can view the imported routes.

```
[SwitchA] display ospf routing

          OSPF Process 1 with Router ID 192.168.1.1
                  Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.1.0/24     1  Stub       192.168.1.1     192.168.1.1     0.0.0.0

 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop         AdvRouter
 192.168.2.0/24     1         Type2      1           192.168.1.2     192.168.1.2
 172.17.1.0/24      1         Type2      1           192.168.1.2     192.168.1.2
 172.17.2.0/24      1         Type2      1           192.168.1.2     192.168.1.2
 172.17.3.0/24      1         Type2      1           192.168.1.2     192.168.1.2

 Routing for NSSAs
 Destination        Cost      Type       Tag         NextHop         AdvRouter

 Total Nets: 5
 Intra Area: 1  Inter Area: 0  ASE: 4  NSSA: 0
```

5. Set the filtering list.

   # Set ACL 2002 to match 172.17.2.0/24.

   ```
   [SwitchB] acl number 2002
   [SwitchB-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
   [SwitchB-acl-basic-2002] quit
   ```

   # Set an IP prefix list named prefix-a to match 172.17.1.0/24.

   ```
   [SwitchB] ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
   ```

6. Set a Route-Policy.

   ```
   [SwitchB] route-policy isis2ospf permit node 10
   [SwitchB-route-policy] if-match ip-prefix prefix-a
   [SwitchB-route-policy] apply cost 100
   [SwitchB-route-policy] quit
   [SwitchB] route-policy isis2ospf permit node 20
   [SwitchB-route-policy] if-match acl 2002
   [SwitchB-route-policy] apply tag 20
   [SwitchB-route-policy] quit
   ```

7. Apply the Route-Policy when routes are imported.

   # Configure Switch-B and apply the Route-Policy when routes are imported.

   ```
   [SwitchB] ospf
   [SwitchB-ospf-1] import-route isis 1 route-policy isis2ospf
   [SwitchB-ospf-1] quit
   ```

   # Check the OSPF routing table of SwitchA. You can view the cost of the route with the destination address as 172.17.1.0/24 is 100, and the tag of the route with the destination address as 172.17.2.0/24 is 20. Other routing attributes do not change.

   ```
   [SwitchA] display ospf routing

             OSPF Process 1 with Router ID 192.168.1.1
                     Routing Tables
    Routing for Network
    Destination        Cost  Type       NextHop         AdvRouter       Area
    192.168.1.0/24     1     Stub      192.168.1.1     192.168.1.1     0.0.0.0

    Routing for ASEs
    Destination        Cost      Type       Tag         NextHop          AdvRouter
    192.168.2.0/24     1         Type2      1           192.168.1.2     192.168.1.2
    172.17.1.0/24      100       Type2      1           192.168.1.2     192.168.1.2
    172.17.2.0/24      1         Type2      20          192.168.1.2     192.168.1.2
    172.17.3.0/24      1         Type2      1           192.168.1.2     192.168.1.2
   ```

```
 Routing for NSSAs
 Destination        Cost      Type       Tag         NextHop         AdvRouter

 Total Nets: 5
 Intra Area: 1  Inter Area: 0  ASE: 4  NSSA: 0
```

Configuration Files

- Configuration file of Switch-A

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of Switch-B

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
acl number 2002
 rule 5 permit source 172.17.2.0 0.0.0.255
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
ospf 1
 import-route isis 1 route-policy isis2ospf
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
route-policy isis2ospf permit node 10
 if-match ip-prefix prefix-a
 apply cost 100
#
route-policy isis2ospf permit node 20
 if-match acl 2002
 apply tag 20
#
return
```

- Configuration file of Switch-C

```
#
 sysname SwitchC
#
 vlan batch 20 30 40 50
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0001.00
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif30
 ip address 172.17.1.1 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 172.17.2.1 255.255.255.0
 isis enable 1
#
interface Vlanif50
 ip address 172.17.3.1 255.255.255.0
 isis enable 1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 40
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 50
#
return
```

3.10 MCE Configuration

Generally, a Customer Edge (CE) can connect to only one Virtual Private Network (VPN). If multiple VPNs need to be divided, multiple CEs are required. The Multi-VPN-Instance CE (MCE) technology enables a CE to be connected to multiple VPNs. This isolates services between different VPNs and reduces the investment on network devices.

3.10.1 Example for Configuring MCE

Networking Requirements

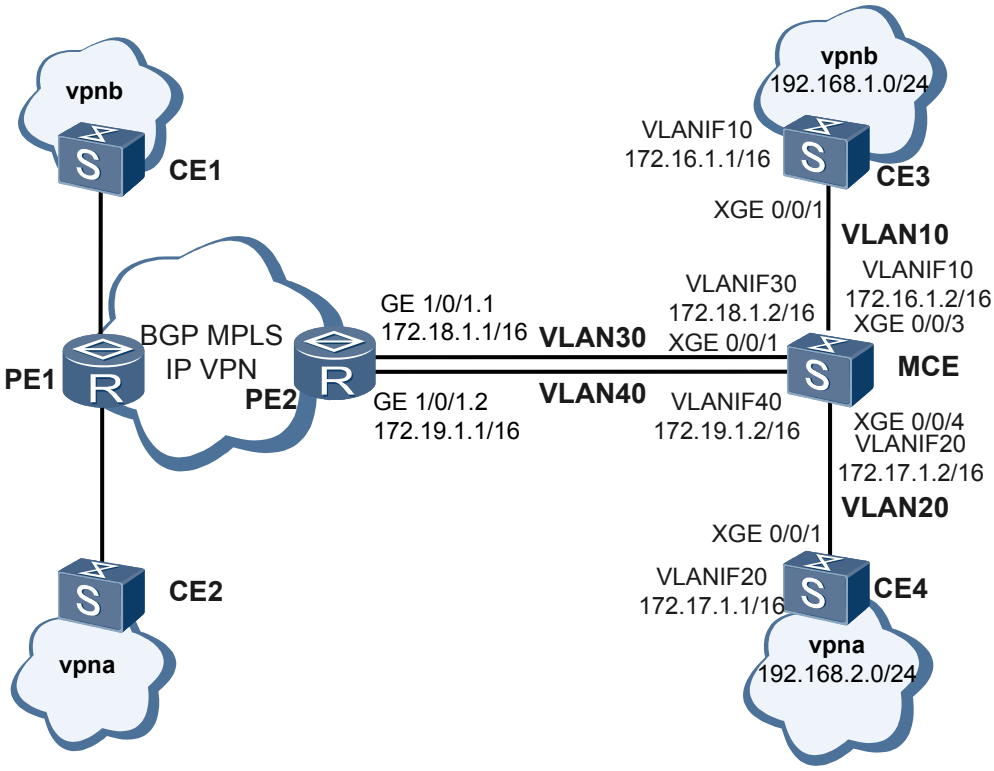
As shown in **Figure 3-26**, the networking is as follows:

- CE1, CE2, CE3, and CE4 are edge devices of the VPN.
- CE1 and CE3 belong to a VPN instance named **vpnb**, and CE2 and CE4 belong to a VPN instance named **vpna**.

- PE1 and PE2 are edge routers of the backbone network.BGP or MPLS IP VPN is configured on the backbone network between PE1 and PE2.
- The MCE functions as a Multi-VPN-Instance CE located in the user network.
- RIP is run between the MCE, CE3, and CE4.
- OSPF is run between the MCE and PE2.

It is required that route isolation between VPNs be implemented on the MCE and routes of VPNs be advertised to the PE2 through OSPF.

Figure 3-26 Networking diagram for configuring MCE



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the MCE, PE2, CE3, and CE4, and add the interfaces connecting these devices to the VLANs.
2. Create and configure VPN instances on the MCE and PE2.
3. Configure the OSPF route multi-instance on the MCE and PE2.
4. Configure RIP between the MCE and CE3, and between the MCE and CE4.

Data Preparation

To complete the configuration, you need the following data:

- VLANs between the MCE, PE2, CE3, and CE4, as shown in **Figure 3-26**

- IP addresses of VLANIF interfaces, as shown in **Figure 3-26**

Configuration Procedure

1. Create VLANs on the MCE, PE2, CE3, and CE4, and add the interfaces connecting these devices to the VLANs.

   # Create VLANs on the MCE.

   ```
   <Quidway> system-view
   [Quidway] sysname MCE
   [MCE] vlan batch 10 20 30 40
   ```

   # Add interfaces to the VLANs on the MCE.

   ```
   [MCE] interface xgigabitethernet 0/0/1
   [MCE-XGigabitEthernet0/0/1] port link-type trunk
   [MCE-XGigabitEthernet0/0/1] port trunk allow-pass vlan 30 40
   [MCE-XGigabitEthernet0/0/1] quit
   [MCE] interface xgigabitethernet 0/0/3
   [MCE-XGigabitEthernet0/0/3] port link-type trunk
   [MCE-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
   [MCE-XGigabitEthernet0/0/3] quit
   [MCE] interface xgigabitethernet 0/0/4
   [MCE-XGigabitEthernet0/0/4] port link-type trunk
   [MCE-XGigabitEthernet0/0/4] port trunk allow-pass vlan 20
   [MCE-XGigabitEthernet0/0/4] quit
   ```

   # Create sub-interfaces on PE2 and add these sub-interfaces to the VLAN.

   ```
   <Quidway> system-view
   [Quidway] sysname PE2
   [PE2] interface gigabitethernet 1/0/1.1
   [PE2-GigabitEthernet1/0/1.1] vlan-type dot1q 30
   [PE2-GigabitEthernet1/0/1.1] quit
   [PE2] interface gigabitethernet 1/0/1.2
   [PE2-GigabitEthernet1/0/1.2] vlan-type dot1q 40
   [PE2-GigabitEthernet1/0/1.2] quit
   ```

   # Create a VLAN on CE3.

   ```
   <Quidway> system-view
   [Quidway] sysname CE3
   [CE3] vlan 10
   ```

   # Add an interface to the VLAN on CE3.

   ```
   [CE3-A] interface xgigabitethernet 0/0/1
   [CE3-XGigabitEthernet0/0/1] port link-type trunk
   [CE3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
   [CE3-XGigabitEthernet0/0/1] quit
   ```

   # Create a VLAN on CE4.

   The configuration on CE4 is similar to that on CE3, and is not mentioned here.

   # Add an interface to the VLAN on CE4.

   The configuration on CE4 is similar to that on CE3, and is not mentioned here.

2. Create and configure VPN instances.

   # Create VPN instances on the MCE.

   ```
   [MCE] ip vpn-instance vpna
   [MCE-vpn-instance-vpna] route-distinguisher 100:1
   [MCE-vpn-instance-vpna] quit
   [MCE] ip vpn-instance vpnb
   [MCE-vpn-instance-vpnb] route-distinguisher 100:2
   [MCE-vpn-instance-vpnb] quit
   ```

   # Bind VPN instances to VLANIF interfaces on the MCE and assign IP addresses to the VLANIF interfaces.

   ```
   [MCE] interface vlanif 10
   [MCE-Vlanif10] ip binding vpn-instance vpnb
   ```

```
[MCE-Vlanif10] ip address 172.16.1.2 16
[MCE-Vlanif10] quit
[MCE] interface vlanif 20
[MCE-Vlanif20] ip binding vpn-instance vpna
[MCE-Vlanif20] ip address 172.17.1.2 16
[MCE-Vlanif20] quit
[MCE] interface vlanif 30
[MCE-Vlanif30] ip binding vpn-instance vpnb
[MCE-Vlanif30] ip address 172.18.1.2 16
[MCE-Vlanif30] quit
[MCE] interface vlanif 40
[MCE-Vlanif40] ip binding vpn-instance vpna
[MCE-Vlanif40] ip address 172.19.1.2 16
[MCE-Vlanif40] quit
```

Create VPN instances on PE2.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 100:1
[PE2-vpn-instance-vpna] quit
[PE2] ip vpn-instance vpnb
[PE2-vpn-instance-vpnb] route-distinguisher 100:2
[PE2-vpn-instance-vpnb] quit
```

Bind VPN instances to sub-interfaces on PE2 and assign IP addresses to the sub-interfaces.

```
[PE2] interface gigabitethernet 1/0/1.1
[PE2-GigabitEthernet1/0/1.1] ip binding vpn-instance vpnb
[PE2-GigabitEthernet1/0/1.1] ip address 172.18.1.1 255.255.0.0
[PE2-GigabitEthernet1/0/1.1] quit
[PE2] interface gigabitethernet 1/0/1.2
[PE2-GigabitEthernet1/0/1.2] ip binding vpn-instance vpna
[PE2-GigabitEthernet1/0/1.2] ip address 172.19.1.1 255.255.0.0
[PE2-GigabitEthernet1/0/1.2] quit
```

3. Configure the OSPF route multi-instance between the MCE and PE2.

   # Configure the OSPF route multi-instance on PE2.

```
[PE2] ospf 100 vpn-instance vpna
[PE2-ospf-100] area 0
[PE2-ospf-100-area-0.0.0.0] network 172.19.0.0 0.0.255.255
[PE2-ospf-100-area-0.0.0.0] quit
[PE2-ospf-100] quit
[PE2] ospf 200 vpn-instance vpnb
[PE2-ospf-200] area 0
[PE2-ospf-200-area-0.0.0.0] network 172.18.0.0 0.0.255.255
[PE2-ospf-200-area-0.0.0.0] quit
[PE2-ospf-200] quit
```

   # Configure the OSPF route multi-instance on the MCE.

```
[MCE] ospf 100 vpn-instance vpna
[MCE-ospf-100] area 0
[MCE-ospf-100-area-0.0.0.0] network 172.19.0.0 0.0.255.255
[MCE-ospf-100-area-0.0.0.0] quit
[MCE-ospf-100] quit
[MCE] ospf 200 vpn-instance vpnb
[MCE-ospf-200] area 0
[MCE-ospf-200-area-0.0.0.0] network 172.18.0.0 0.0.255.255
[MCE-ospf-200-area-0.0.0.0] return
```

4. Configure RIP between the MCE and CE3, and between the MCE and CE4.

   # Configure RIP-2 on the MCE.

```
[MCE] rip 100 vpn-instance vpna
[MCE-rip-100] version 2
[MCE-rip-100] network 172.17.0.0
[MCE-rip-100] import-route ospf 100
[MCE-rip-100] quit
[MCE] rip 200 vpn-instance vpnb
[MCE-rip-200] version 2
```

```
[MCE-rip-200] network 172.16.0.0
[MCE-rip-200] import-route ospf 200
```

Configure RIP-2 on CE3.

```
[CE3] rip 200
[CE3-rip-200] version 2
[CE3-rip-200] network 172.16.0.0
[CE3-rip-200] network 192.168.1.0
[CE3-rip-200] import-route direct
```

Configure RIP-2 on CE4.

```
[CE4] rip 100
[CE4-rip-100] version 2
[CE4-rip-100] network 172.17.0.0
[CE4-rip-100] network 192.168.2.0
[CE4-rip-100] import-route direct
```

Import RIP routes on the MCE.

```
[MCE] ospf 100
[MCE-ospf-100] import-route rip 100
[MCE-ospf-100] quit
[MCE] ospf 200
[MCE-ospf-200] import-route rip 200
```

5. Verify the configuration.

   # After the configuration, run the **display ip routing-table vpn-instance** command on the MCE, and you can view the routes to the local VPN.

   Take **vpnb** as an example:

```
[MCE] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: vpnb
         Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

     172.16.0.0/16  Direct 0    0           D  172.16.1.2      Vlanif10
     172.16.1.1/32  Direct 0    0           D  172.16.1.1      Vlanif10
     172.16.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
     172.18.0.0/16  Direct 0    0           D  172.18.1.2      Vlanif30
     172.18.1.1/32  Direct 0    0           D  172.18.1.1      Vlanif30
     172.18.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
     192.168.0.0/16  RIP   100  1           D  172.16.1.1      Vlanif10
```

Configuration Files

- Configuration file of the MCE

```
#
 sysname MCE
#
 vlan batch 10 20 30 40
#
ip vpn-instance vpna
 route-distinguisher 100:1
#
ip vpn-instance vpnb
 route-distinguisher 100:2
#
interface Vlanif10
 ip binding vpn-instance vpnb
 ip address 172.16.1.2 255.255.0.0
#
interface Vlanif20
 ip binding vpn-instance vpna
 ip address 172.17.1.2 255.255.0.0
#
```

```
interface Vlanif30
 ip binding vpn-instance vpnb
 ip address 172.18.1.2 255.255.0.0
#
interface Vlanif40
 ip binding vpn-instance vpna
 ip address 172.19.1.2 255.255.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30 40
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 20
#
ospf 100 vpn-instance vpna
 import-route rip 100
 area 0.0.0.0
  network 172.17.0.0 0.0.255.255
  network 172.19.0.0 0.0.255.255
#
ospf 200 vpn-instance vpnb
 import-route rip 200
 area 0.0.0.0
  network 172.16.0.0 0.0.255.255
  network 172.18.0.0 0.0.255.255
#
rip 100 vpn-instance vpna
 version 2
 network 172.17.0.0
 import-route ospf 100
#
rip 200 vpn-instance vpnb
 version 2
 network 172.16.0.0
 import-route ospf 200
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
ip vpn-instance vpna
 route-distinguisher 100:1
#
ip vpn-instance vpnb
 route-distinguisher 100:2
#
interface GigabitEthernet1/0/1.1
 vlan-type dot1q 30
 ip binding vpn-instance vpnb
 ip address 172.18.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1.2
 vlan-type dot1q 40
 ip binding vpn-instance vpna
 ip address 172.19.1.1 255.255.0.0
#
#
ospf 100 vpn-instance vpna
 area 0.0.0.0
  network 172.19.0.0 0.0.255.255
#
ospf 200 vpn-instance vpnb
```

```
 area 0.0.0.0
  network 172.18.0.0 0.0.255.255
#
return
```

NOTE

The following lists only configuration files related to the MCE. For details on configuring BGP or MPLS IP VPN, refer to manuals of corresponding devices.

- Configuration file of CE3

```
#
 sysname CE3
#
vlan batch 10
#
interface Vlanif10
 ip address 172.16.1.1 255.255.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
rip 200
 version 2
 network 172.16.0.0
 network 192.168.1.0
 import-route direct
#
return
```

- Configuration file of CE4

```
#
 sysname CE4
#
vlan batch 20
#
interface Vlanif20
 ip address 172.17.1.1 255.255.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
rip 100
 version 2
 network 172.17.0.0
 network 192.168.2.0
 import-route direct
#
return
```

4 Configuration Guide - Multicast

About This Chapter

This document describes the multicast service supported by the S6700, including basic knowledge, protocol implementation, configuration procedures, and configuration examples.

This document guides you through the configuration of the multicast service of the S6700.

4.1 IGMP Snooping Configuration
This chapter describes the procedure for configuring IGMP snooping and maintenance commands, and provides configuration examples.

4.2 Multicast VLAN Replication Configuration
This chapter describes the procedure for configuring multicast VLAN replication and maintenance commands, and provides configuration examples.

4.3 Controllable Multicast Configuration
This chapter describes the principle of controllable multicast and procedures for configuring controllable multicast.

4.4 IGMP Configuration
This chapter describes the procedure for configuring IGMP and commands for maintaining IGMP, and provides configuration examples.

4.5 PIM-DM (IPv4) Configuration
This chapter describes the PIM-DM (IPv4) fundamentals, configuration steps, and maintenance for PIM-DM functions, along with typical examples.

4.6 PIM-SM (IPv4) Configuration
The PIM protocol is used to implement multicast routing and data forwarding inside an AS. The PIM-SM protocol is a multicast routing protocol of sparse node. It is applicable to a large-scale network with sparsely-distributed members.

4.7 MSDP Configuration
The MSDP protocol is used to implement multicast routing and data forwarding between PIM-SM domains and anycast RP in a PIM-SM domain.

4.8 IPv4 Multicast Routing Management
The system synchronously maintains multiple multicast routing protocols, and controls multicast routing and forwarding through the information exchanged between the control plane and the forwarding plane.

4.9 MLD Snooping Configuration

This chapter describes the implementation and configuration procedures of Multicast Listener Discovery (MLD) snooping on the S6700.

4.1 IGMP Snooping Configuration

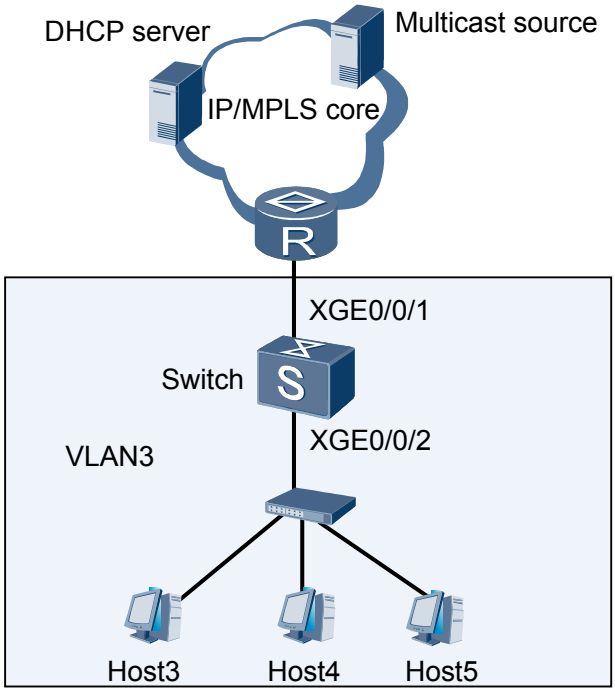
This chapter describes the procedure for configuring IGMP snooping and maintenance commands, and provides configuration examples.

4.1.1 Example for Configuring IGMP Snooping

Networking Requirements

As shown in **Figure 4-1**, XGE 0/0/1 of the S6700 is connected to a router on the multicast source side, and XGE 0/0/2 is connected to hosts. You are required to configure IGMP snooping to ensure that three hosts in VLAN 3 can receive multicast data from multicast groups in the range of 225.1.1.1 to 225.1.1.3 permanently.

Figure 4-1 Networking diagram for configuring VLAN-based IGMP snooping



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and add interfaces to the VLAN.
2. Enable IGMP snooping globally and in the VLAN.
3. Configure a static router interface.
4. Configure static multicast groups 225.1.1.1, 225.1.1.2, and 225.1.1.3.

Data Preparation

To complete the configuration, you need the following data:

- ID of the VLAN that XGE 0/0/2 and XGE 0/0/1 belong to: VLAN 3
- Static router interface: XGE0/0/1
- Addresses of static multicast groups: 225.1.1.1, 225.1.1.2, 225.1.1.3

Procedure

Step 1 Create a VLAN and add interfaces to the VLAN.

```
<Switch> system-view
[Switch] vlan 3
[Switch-vlan3] quit
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] port hybrid tagged vlan 3
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet 0/0/2
[Switch-XGigabitEthernet0/0/2] port hybrid tagged vlan 3
[Switch-XGigabitEthernet0/0/2] quit
```

Step 2 Enable IGMP snooping.

Enable IGMP snooping globally.

```
[Switch] igmp-snooping enable
```

Enable IGMP snooping in VLAN 3.

```
[Switch] vlan 3
[Switch-vlan3] igmp-snooping enable
[Switch-vlan3] quit
```

Step 3 Configure XGE 0/0/1 as the static router interface of VLAN 3.

```
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] igmp-snooping static-router-port vlan 3
[Switch-XGigabitEthernet0/0/1] quit
```

Step 4 Configure static multicast groups.

```
[Switch] interface xgigabitethernet 0/0/2
[Switch-XGigabitEthernet0/0/2] l2-multicast static-group group-address 225.1.1.1
vlan 3
[Switch-XGigabitEthernet0/0/2] l2-multicast static-group group-address 225.1.1.2
vlan 3
[Switch-XGigabitEthernet0/0/2] l2-multicast static-group group-address 225.1.1.3
vlan 3
[Switch-XGigabitEthernet0/0/2] quit
```

Step 5 Verify the configuration.

Check all configurations of IGMP snooping.

```
[Switch] display igmp-snooping vlan configuration
IGMP Snooping Configuration for VLAN 3
     igmp-snooping enable
```

According to the preceding information, the IGMP snooping of the VLAN is enabled.

Check the configuration of the static router interface.

Run the **display igmp-snooping router-port vlan 3** command on the S6700.

```
[Switch] display igmp-snooping router-port vlan 3
 Port Name                 UpTime    Expires   Flags
```

```
 ------------------------------------------------------------------------
 VLAN 3, 1 router-port(s)
 XGE0/0/1                  2d:10h     --       STATIC
```

According to the preceding information, XGE 0/0/1 is configured as a static router interface.

Verify the information about member interfaces of a static multicast group.

```
[Switch] display igmp-snooping port-info
 ------------------------------------------------------------------------
                     (Source, Group)  Port                           Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ------------------------------------------------------------------------
 VLAN 3, 3 Entry(s)
                      (*, 225.1.1.1)  XGE0/0/2                        S--
                                                  1 port(s)
                      (*, 225.1.1.2)  XGE0/0/2                        S--
                                                  1 port(s)
                      (*, 225.1.1.3)  XGE0/0/2                        S--
                                                  1 port(s)
 ------------------------------------------------------------------------
```

According to the preceding information, multicast groups 225.1.1.1 to 225.1.1.3 are configured with static forwarding entries.

View the multicast forwarding table.

```
[Switch] display l2-multicast forwarding-table vlan 3

VLAN ID : 3, Forwarding Mode : IP
------------------------------------------------------------------------
                     (Source, Group)    Interface             Out-Vlan
------------------------------------------------------------------------
                        Router-port     XGigabitEthernet0/0/1     3
                      (*, 225.1.1.1)    XGigabitEthernet0/0/1     3
                                        XGigabitEthernet0/0/2     3
                      (*, 225.1.1.2)    XGigabitEthernet0/0/1     3
                                        XGigabitEthernet0/0/2     3
                      (*, 225.1.1.3)    XGigabitEthernet0/0/1     3
                                        XGigabitEthernet0/0/2     3
------------------------------------------------------------------------
Total Group(s) : 3
```

The preceding information shows the VLAN ID and outgoing interface mapping the data from multicast groups 225.1.1.1 to 225.1.1.3.

----End

Configuration Files

- Configuration file of the S6700

```
#
 sysname Switch
#
 vlan batch 3
#
 igmp-snooping enable
#
vlan 3
 igmp-snooping enable
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 3
 igmp-snooping static-router-port vlan 3
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 3
```

```
l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 3
#
return
```

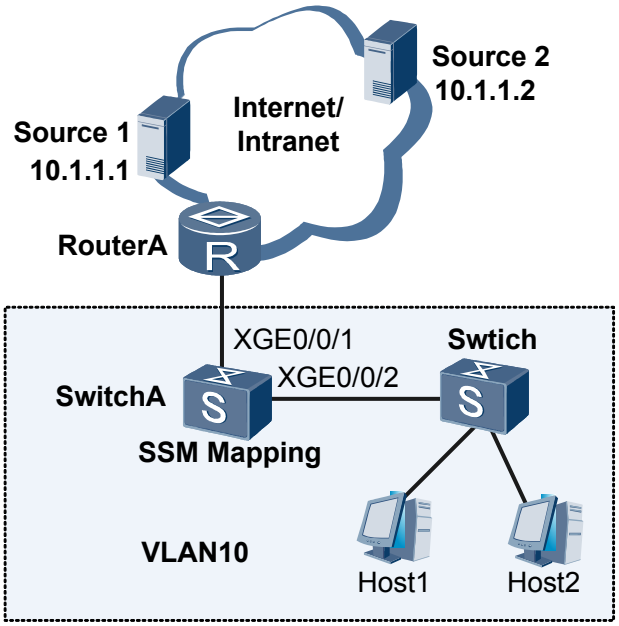
4.1.2 Example for Configuring IGMP Snooping SSM Mapping

Networking Requirements

On the network shown in **Figure 4-2**, IGMPv2 is run on Switch and Host 1 and Host 2, and IGMPv3 is run on the last-hop router Router A on the multicast source side. Switch A is the S6700 device. XGE 0/0/1 on Switch A is connected to Router A and XGE 0/0/2 on Switch A is connected to a switch directly connected with users. XGE 0/0/1 on Switch A is a static router interface and XGE 0/0/2 is statically added to multicast group 224.1.1.1. XGE 0/0/1 and XGE 0/0/2 both join VLAN 10 and IGMP SSM mapping is deployed on Router A.

It is required that IGMP snooping SSM mapping be configured on Switch A in the VLAN to work jointly with IGMP SSM mapping. IGMP snooping SSM mapping also generates a mapping between a multicast group and a multicast source. (*, G) information in IGMPv1 or IGMPv2 multicast data packets is then mapped to (S, G) information, providing SSM services for the hosts running IGMPv1 or IGMPv2.

Figure 4-2 Networking diagram for configuring IGMP snooping SSM mapping



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic IGMP snooping functions so that users can receive multicast data from multicast sources.
2. Configure an SSM group policy for IGMP snooping to add the ASM group addresses of users to the SSM group address range.

3. Configure IGMP snooping SSM mapping so that users can receive multicast data from a specified multicast source.

Data Preparation

To complete the configuration, you need the following data:

- VLAN 10 to which XGE 0/0/1 and XGE 0/0/2 on Switch A are added
- IGMPv3 run on Switch A and IGMPv2 run on Switch, Host 1, and Host 2
- Multicast source address 10.1.1.2

Procedure

Step 1 Configure a VLAN.

Configure Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/2] quit
```

Step 2 Enable global IGMP snooping and IGMP snooping in the VLAN.

Configure Switch A.

```
[SwitchA] igmp-snooping enable
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping enable
```

Step 3 Configure IGMPv3 on Switch A and configure IGMPv2 on hosts. The hosts are not allowed to upgrade the IGMP version to 3.

Configure SwitchA.

```
[SwitchA-vlan10] igmp-snooping version 3
[SwitchA-vlan10] quit
```

Step 4 Configure XGE 0/0/1 as a static router interface in VLAN 10.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] igmp-snooping static-router-port vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
```

Step 5 Configure an SSM group policy for IGMP snooping and enable IGMP snooping SSM mapping.

```
[SwitchA] acl number 2008
[SwitchA-acl-basic-2008] rule 5 permit source 224.1.1.1 0
[SwitchA-acl-basic-2008] quit
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping ssm-policy 2008
[SwitchA-vlan10] igmp-snooping ssm-mapping enable
[SwitchA-vlan10] igmp-snooping ssm-mapping 224.1.1.1 24 10.1.1.2
[SwitchA-vlan10] quit
```

Step 6 Verify the configuration.

Run the **display igmp-snooping vlan configuration** command on Switch A. You can view IGMP snooping configurations in the VLAN.

```
[SwitchA] display igmp-snooping vlan configuration
 IGMP Snooping Configuration for VLAN 10
     igmp-snooping enable
     igmp-snooping version 3
     igmp-snooping ssm-mapping enable
     igmp-snooping ssm-policy 2008
     igmp-snooping ssm-mapping 224.1.1.0 255.255.255.0 10.1.1.2
```

After SwitchA receives a Report message, run the **display igmp-snooping port-info** command to view the configurations on the interface.

```
[SwitchA] display igmp-snooping port-info
 ----------------------------------------------------------------------------
                     (Source, Group)  Port                              Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------------
 VLAN 10, 1 Entry(s)
                       (10.1.1.2, 224.1.1.1)  XGE0/0/2                --M
                                                        1 port(s)
 ----------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10
#
 igmp-snooping enable
#
acl number 2008
 rule 5 permit source 224.1.1.1 0
#
vlan 10
 igmp-snooping enable
 igmp-snooping ssm-mapping enable
 igmp-snooping version 3
 igmp-snooping ssm-policy 2008
 igmp-snooping ssm-mapping 224.1.1.0 255.255.255.0 10.1.1.2
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 igmp-snooping static-router-port vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

4.2 Multicast VLAN Replication Configuration

This chapter describes the procedure for configuring multicast VLAN replication and maintenance commands, and provides configuration examples.

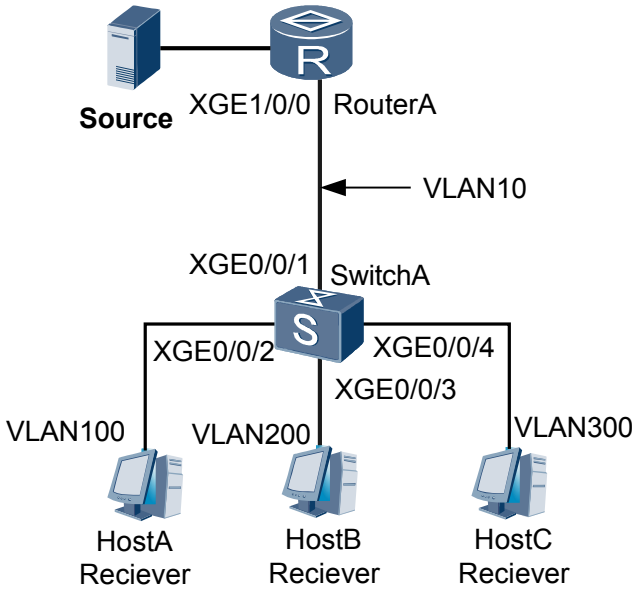
4.2.1 Example for Configuring Multicast VLAN Replication Based on User VLANs

Networking Requirements

As shown in **Figure 4-3**, RouterA is connected to the multicast source. XGE 1/0/0 of RouterA is connected to XGE0/0/1 of SwitchA. XGE0/0/1 of SwitchA belongs to VLAN 10. HostA, HostB, and HostC are connected to XGE0/0/2, XGE0/0/3, and XGE0/0/4 of SwitchA and belong to VLAN 100, VLAN 200, and VLAN 300 respectively.

To save network bandwidth, you can configure multicast VLAN replication based on user VLANs on SwitchA. RouterA then only needs to send one copy of multicast data to the multicast VLAN, and SwitchA distributes multicast data to user VLANs.

Figure 4-3 Networking diagram for configuring multicast VLAN replication based on user VLANs



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IGMP snooping globally.
2. Create a multicast VLAN and enable IGMP snooping in the multicast VLAN.
3. Create user VLANs and enable IGMP snooping in the user VLANs.
4. Bind the user VLANs to the multicast VLAN.
5. Add the network-side interface and user-side interfaces to VLANs as hybrid interfaces.

Data Preparation

To complete the configuration, you need the following data:

- Interface connected to RouterA and the VLAN that the interface belongs to
- User-side interfaces and the VLANs that the interfaces belong to

Procedure

Step 1 Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
```

Step 2 Create a multicast VLAN and enable IGMP snooping in the multicast VLAN.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] multicast-vlan enable
[SwitchA-vlan10] quit
```

Step 3 Create user VLANs and enable IGMP snooping in the user VLANs.

```
[SwitchA] vlan 100
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] igmp-snooping enable
[SwitchA-vlan200] quit
[SwitchA] vlan 300
[SwitchA-vlan300] igmp-snooping enable
[SwitchA-vlan300] quit
```

Step 4 Bind user VLANs 100, 200, and 300 to multicast VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] multicast-vlan user-vlan 100 200 300
[SwitchA-vlan10] quit
```

Step 5 Add interfaces to VLANs as hybrid interfaces.

Add XGE0/0/1 to multicast VLAN 10.

```
[SwitchA] interface xgigabitethernet0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
```

Add XGE0/0/2, XGE0/0/3, and XGE0/0/4 to user VLANs 100, 200, and 300 respectively.

```
[SwitchA] interface xgigabitethernet0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid pvid vlan 100
[SwitchA-XGigabitEthernet0/0/2] port hybrid untagged vlan 100
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface xgigabitethernet0/0/3
[SwitchA-XGigabitEthernet0/0/3] port hybrid pvid vlan 200
[SwitchA-XGigabitEthernet0/0/3] port hybrid untagged vlan 200
[SwitchA-XGigabitEthernet0/0/3] quit
[SwitchA] interface xgigabitethernet0/0/4
[SwitchA-XGigabitEthernet0/0/4] port hybrid pvid vlan 300
[SwitchA-XGigabitEthernet0/0/4] port hybrid untagged vlan 300
[SwitchA-XGigabitEthernet0/0/4] quit
```

Step 6 Verify the configuration.

View information about the multicast VLAN and user VLANs on SwitchA.

```
[SwitchA] display multicast-vlan vlan
Total multicast vlan   1
 multicast-vlan     user-vlan number     snooping-state
 ------------------------------------------------------------
 10                 3                   IGMP Enable /MLD Disable
[SwitchA] display user-vlan vlan
 Total user vlan   3
 user-vlan  snooping-state            multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 100        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 200        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 300        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
```

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 10 100 200 300
#
 igmp-snooping enable
#
vlan 10
 igmp-snooping enable
 multicast-vlan enable
 multicast-vlan user-vlan 100 200 300
#
vlan 100
 igmp-snooping enable
#
vlan 200
 igmp-snooping enable
#
vlan 300
 igmp-snooping enable
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/4
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
return
```

4.2.2 Example for Configuring Multicast VLAN Replication Based on Interfaces

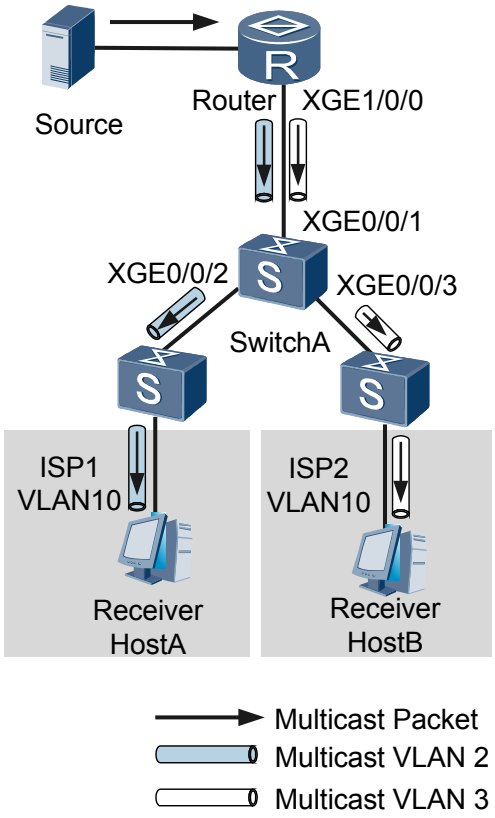
Networking Requirements

As shown in **Figure 4-4**, the Router is connected to the multicast source. XGE 0/0/1 of the Switch A is connected to the Router. XGE 0/0/2 provides services for ISP1, and XGE 0/0/3 provides

services for ISP2. ISP1 and ISP2 use multicast VLAN 2 and VLAN 3 respectively to provide multicast services for users. XGE 0/0/2 and XGE 0/0/3 belong to user VLAN 10.

To protect interests of the ISPs and ensure that multicast packets of each ISP are only sent to users of the ISP, multicast VLANs and user VLANs can be bound on the user-side interfaces. After the configuration is complete, multicast data of an ISP will be sent only to the interface connected to the ISP.

Figure 4-4 Networking diagram for configuring multicast VLAN replication based on interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IGMP snooping globally.
2. Create multicast VLANs 2 and 3 and enable IGMP snooping in the multicast VLANs.
3. Create user VLAN 10.
4. Bind the user VLAN to multicast VLANs on XGE 0/0/2 and XGE 0/0/3.
5. Add the network-side interface and user-side interfaces to VLANs as hybrid interfaces.

Data Preparation

To complete the configuration, you need the following data:

- Interface connected to the Router and the VLAN that the interface belongs to

- User-side interfaces and the VLANs that the interfaces belong to

Procedure

Step 1 Create multicast VLANs 2 and 3 and enable IGMP snooping in the multicast VLANs.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] igmp-snooping enable
[SwitchA-vlan3] quit
```

Step 2 Create user VLAN 10.

```
[Switch] vlan batch 10
```

Step 3 Bind the user VLAN to multicast VLANs on XGE 0/0/2 and XGE 0/0/3.

```
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] l2-multicast-bind vlan 10 mvlan 2
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] l2-multicast-bind vlan 10 mvlan 3
[SwitchA-XGigabitEthernet0/0/3] quit
```

Step 4 Add XGE0/0/1 to the multicast VLANs, and add XGE 0/0/2 and XGE 0/0/3 to the user VLAN.

Add XGE0/0/1 to multicast VLANs 2 and 3 as a trunk interface.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2 3
[SwitchA-XGigabitEthernet0/0/1] quit
```

Add XGE0/0/2 and XGE0/0/3 to VLAN 10 as hybrid interfaces.

```
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/3] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/3] quit
```

Step 5 Verify the configuration.

Run the **display l2-multicast-bind** [**mvlan** *vlan-id*] command on the Switch A to view binding between user VLANs and multicast VLANs.

```
[SwitchA] display l2-multicast-bind
 ------------------------------------------------------------------------
 Port                          Startvlan        Endvlan        Mvlan
 ------------------------------------------------------------------------
 XGigabitEthernet0/0/2         10             --            2
 XGigabitEthernet0/0/3         10             --            3
 ------------------------------------------------------------------------
 Total Table(s) : 2
```

----End

Configuration Files

- Configuration file of the SwitchA

```
#
 sysname Switch
```

```
#
 vlan batch 2 3 10
#
 igmp-snooping enable
#
vlan 2
 igmp-snooping enable
#
vlan 3
 igmp-snooping enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 3
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast-bind vlan 10 mvlan 2
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast-bind vlan 10 mvlan 3
#
return
```

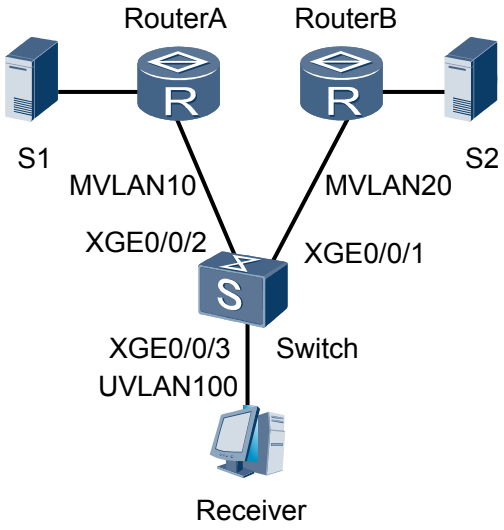
4.2.3 Example for Configuring Many-to-Many Multicast VLANs

Networking Requirements

As shown in **Figure 4-5**, XGE 0/0/1 of Switch is connected to Router A and receives multicast data from Router A through multicast VLAN 10.XGE 0/0/2 of Switch is connected to Router B and receives multicast data from Router B through multicast VLAN 20. XGE 0/0/3 of Switch is connected to the user VLAN.

The user needs to receive data of multicast group 225.1.1.1 from Router A and receive data of multicast group 225.1.2.1 from Router B.

Figure 4-5 Networking diagram of many-to-many multicast VLAN replication based on user VLANs



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IGMP snooping in the system view.
2. Create multicast VLANs and enable IGMP snooping in the multicast VLAN.
3. Create a user VLAN and enable IGMP snooping in the user VLAN. Enable the triggering of the multicast flow in the user VLAN.
4. Add the user VLAN to multiple multicast VLANs and configure the static multicast flow in the multicast VLANs.
5. Add the network-side interfaces and user-side interface to VLANs as hybrid interfaces.

Data Preparation

To complete the configuration, you need the following data:

- Interfaces connected to the routers and the multicast VLANs that the interfaces belong to
- Interfaces connected to the user and the multicast VLANs that the interfaces belong to

Procedure

Step 1 Enable IGMP snooping in the system view.

```
<Switch> system-view
[Switch] igmp-snooping enable
```

Step 2 Create multicast VLANs 10 and 20 and enable IGMP snooping in the multicast VLANs.

```
[Switch] igmp-snooping enable
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] multicast-vlan enable
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] igmp-snooping enable
[Switch-vlan20] multicast-vlan enable
[Switch-vlan20] quit
```

Step 3 Create user VLAN 100 and enable IGMP snooping in the user VLAN. Enable the triggering of the multicast flow in the user VLAN.

```
[Switch] vlan 100
[Switch-vlan100] igmp-snooping enable
[Switch-vlan100] multicast flow-trigger enable
[Switch-vlan100] quit
```

Step 4 Add user VLAN 100 to multicast VLANs10 and 20 and configure the static multicast flow in the multicast VLANs.

```
[Switch] vlan 10
[Switch-vlan10] multicast-vlan user-vlan 100
[Switch-vlan10] multicast static-flow 225.1.1.1
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] multicast-vlan user-vlan 100
[Switch-vlan20] multicast static-flow 225.1.2.1
[Switch-vlan20] quit
```

Step 5 Add interfaces to VLANs as hybrid interfaces.

Add XGE 0/0/1 to multicast VLAN 20. Add XGE 0/0/2 to multicast VLAN 10.

```
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] port hybrid pvid vlan 20
[Switch-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet 0/0/2
[Switch-XGigabitEthernet0/0/2] port hybrid pvid vlan 10
[Switch-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[Switch-XGigabitEthernet0/0/2] quit
```

Add XGE 0/0/3 to user VLAN 100.

```
[Switch] interface xgigabitethernet 0/0/3
[Switch-XGigabitEthernet0/0/3] port hybrid pvid vlan 100
[Switch-XGigabitEthernet0/0/3] port hybrid untagged vlan 100
[Switch-XGigabitEthernet0/0/3] quit
```

Step 6 Verify the configuration.

Run the **display user-vlan vlan** command. You can see that the user VLAN has been added to multicast VLANs 10 and 20.

```
[Quidway] display user-vlan vlan
 Total user vlan   2
 user-vlan  snooping-state            multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 100        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 100        IGMP Enable /MLD Disable  20              IGMP Enable /MLD Disable
```

Run the **display multicast static-flow** command to view the static multicast flow in the multicast VLANs. Users in the user VLAN can be added to the multicast group.

```
[Quidway] display multicast static-flow
 ------------------------------------------------------------------
 Vlan                                        (Source, Group)
 ------------------------------------------------------------------
  10                                          (*, 225.1.1.1)
  20                                          (*, 225.1.2.1)
 ------------------------------------------------------------------
 Total Table(s) : 2
```

----End

Configuration File

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 10 20 100
#
 igmp-snooping enable
#
vlan 10
 igmp-snooping
enable
 multicast-vlan
enable
 multicast static-flow 225.1.1.1
 multicast-vlan user-vlan 100
#
vlan 20
 igmp-snooping
enable
 multicast-vlan
enable
 multicast static-flow 225.1.2.1
 multicast-vlan user-vlan 100
#
```

```
vlan 100
 igmp-snooping enable
 multicast flow-trigger enable
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

4.3 Controllable Multicast Configuration

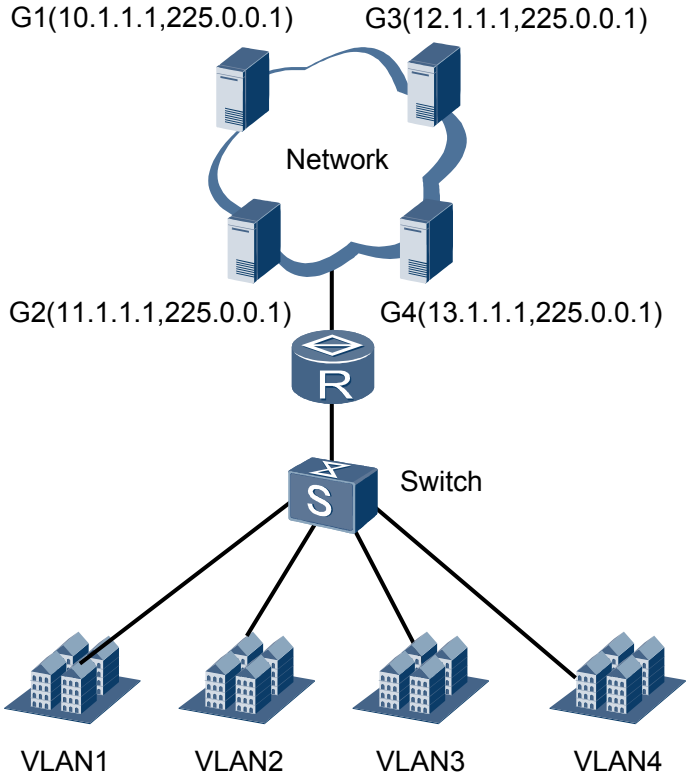
This chapter describes the principle of controllable multicast and procedures for configuring controllable multicast.

4.3.1 Example for Configuring Controllable Multicast

Networking Requirements

As shown in **Figure 4-6**, multicast group G1 (225.0.0.1), G2 (225.0.0.2), G3 (225.0.0.3), and G4 (225.0.0.4) exist in the network connected to the router. You are required to configure users in VLAN 1 and VLAN 2 to watch G1 and G2,and users in VLAN 3 and VLAN 4 to watch all multicast groups.

Figure 4-6 Networking diagram of configuring controllable multicast



Configuration Roadmap

The configuration roadmap is as follows:

- Configure user VLANs.
- Configure IGMP snooping.
- Configure controllable multicast.
  - Two multicast group lists L1 (G1, G2) and L2 (G3, G4)
  - Two multicast profiles P1 and P2

Data Preparation

To complete the configuration, you need the following data:

1. Name of each multicast group
2. Name of each multicast group list
3. Name of each multicast profile

Configuration Procedure

1. Configure user VLANs and add the interface to the user VLANs. The configuration details are not provided here.
2. Configure IGMP snooping.

```
<Switch> system-view
[Switch] igmp-snooping enable
[Switch] vlan 1
[Switch-vlan1] igmp-snooping enable
[Switch-vlan1] quit
[Switch] vlan 2
[Switch-vlan2] igmp-snooping enable
[Switch-vlan2] quit
[Switch] vlan 3
[Switch-vlan3] igmp-snooping enable
[Switch-vlan3] quit
[Switch] vlan 4
[Switch-vlan4] igmp-snooping enable
[Switch-vlan4] quit
```

3. Configure controllable multicast.

   # Configure multicast groups.

```
[Switch] btv
[Switch-btv] multicast-group G1 ip-address 225.0.0.1
[Switch-btv] multicast-group G2 ip-address 225.0.0.2
[Switch-btv] multicast-group G3 ip-address 225.0.0.3
[Switch-btv] multicast-group G4 ip-address 225.0.0.4
```

   # Configure multicast group lists.

```
[Switch-btv] multicast-list L1
[Switch-btv-list-L1] add multicast-group name G1
[Switch-btv-list-L1] add multicast-group name G2
[Switch-btv-list-L1] quit
[Switch-btv] multicast-list L2
[Switch-btv-list-L2] add multicast-group name G3
[Switch-btv-list-L2] add multicast-group name G4
[Switch-btv-list-L2] quit
```

   # Configure multicast profiles.

```
[Switch-btv] multicast-profile P1
[Switch-btv-profile-P1] add multicast-list name L1 watch
[Switch-btv-profile-P1] quit
[Switch-btv] multicast-profile P2
[Switch-btv-profile-P2] add multicast-list name L1 watch
[Switch-btv-profile-P2] add multicast-list name L2 watch
[Quidway-btv-profile-P2] quit
[Quidway-btv] quit
```

   # Apply multicast profiles to VLANs.

```
[Switch] vlan 1
[Switch-vlan1] attach multicast-profile P1
[Switch-vlan1] quit
[Switch] vlan 2
[Switch-vlan2] attach multicast-profile P1
[Switch-vlan2] quit
[Switch] vlan 3
[Switch-vlan3] attach multicast-profile P2
[Switch-vlan3] quit
[Switch] vlan 4
[Switch-vlan4] attach multicast-profile P2
[Switch-vlan4] quit
```

   # Verify the configuration.

```
[Switch-btv] display multicast-profile-apply
--------------------------------------------------------------------------------
  Vlan-id  Port                          SMAC           Max-User Index Profile-
name

--------------------------------------------------------------------------------
  Vlan1    --                            --              8        1    P1
  Vlan2    --                            --              8        1    P1
  Vlan3    --                            --              8        2    P2
  Vlan4    --                            --              8        2    P2
```

```
Total: 4

[Switch-btv] display multicast-profile

--------------------------------------------------------------------------------

 Index        Profile-Name                    Multicast-list  Attach-
User

--------------------------------------------------------------------------------

  1              P1                               1              2
  2              P2                               2              2

 Total: 2
[Switch-btv] display multicast-list

------------------------------------------------------------------------------
 Index        Multicast-list-name             Multicast-
group

------------------------------------------------------------------------------
  1             L1
2
  2             L2
2

 Total: 2

[Switch-btv] display multicast-group
------------------------------------------------------------------------------
 Index        Multicast-group-name
Address

------------------------------------------------------------------------------
  1           G1                                225.0.0.1
  2           G2                                225.0.0.2
  3           G3                                225.0.0.3
  4           G4                                225.0.0.4

 Total: 4
```

Configuration Files

```
 sysname Switch
#
 vlan batch 1 to 4
#
 igmp-snooping enable
#
#
 btv
 multicast-group  G1 ip-address 225.0.0.1
 multicast-group  G2 ip-address 225.0.0.2
 multicast-group  G3 ip-address 225.0.0.3
 multicast-group  G4 ip-address 225.0.0.4
 #
 multicast-list  L1
  add multicast-group name G1
  add multicast-group name G2
 multicast-list  L2
  add multicast-group name G3
  add multicast-group name G4
 #
 multicast-profile  P1
  add  multicast-list name L1 watch
 multicast-profile  P2
  add  multicast-list name L1 watch
```

```
  add  multicast-list name L2 watch
#
vlan 1
 igmp-snooping enable
 attach multicast-profile P1
#
vlan 2
 igmp-snooping enable
 attach multicast-profile P1
#
vlan 3
 igmp-snooping enable
 attach multicast-profile P2
#
vlan 4
 igmp-snooping enable
 attach multicast-profile P2
#
return
```

4.4 IGMP Configuration

This chapter describes the procedure for configuring IGMP and commands for maintaining IGMP, and provides configuration examples.

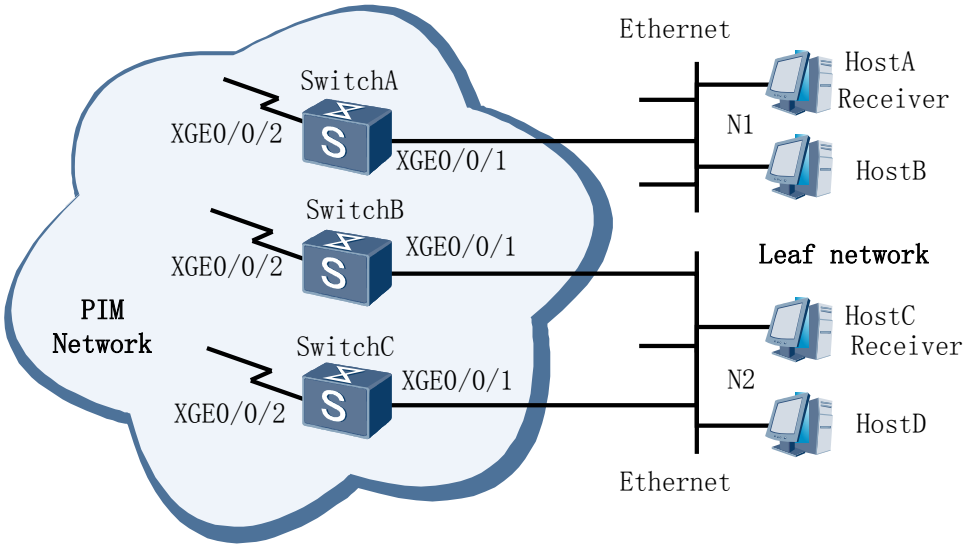
4.4.1 Example for Configuring Basic IGMP Functions

Networking Requirements

On the network as shown in **Figure 4-7**, the unicast routing function is normal. You are required to implement multicast on the network to enable hosts to receive the Video On Demand (VOD) information.

When the hosts connected to a certain interface need to receive a popular program for a long time, you can add the interface to a multicast group statically. As shown in the following figure, if HostA needs to receive the multicast data from the multicast group 225.1.1.1 for a long time, you need to add XGE 0/0/1 on the Switch A to the multicast group 225.1.1.1 statically.

Figure 4-7 Networking diagram for configuring basic IGMP functions



Switch	Physical interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF 10	10.110.1.1/24
	XGE 0/0/2	VLANIF 11	192.168.1.1/24
Switch B	XGE 0/0/1	VLANIF 20	10.110.2.1/24
	XGE 0/0/2	VLANIF 21	192.168.2.1/24
Switch C	XGE 0/0/1	VLANIF 30	10.110.3.1/24
	XGE 0/0/2	VLANIF 31	192.168.3.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable multicast on all switches providing multicast services.
2. Enable PIM-SM on all the interfaces on switch.
3. Enable IGMP on the interfaces on the host side.
4. Add VLANIF 10 on switch to the multicast group 225.1.1.1 statically.

Data Preparation

To complete the configuration, you need the following data:

- Version of IGMP running between switches and hosts
- Static multicast group address: 225.1.1.1

NOTE

This configuration example describes only the commands used to configure IGMP.

Procedure

Step 1 Configure the IP addresses of interfaces and the unicast routing protocol on each switch.

Configure the IP address and mask of each interface according to **Figure 4-7**. Configure OSPF to ensure the communication between Switch A, Switch B, and Switch C on the network layer, and to ensure the dynamic update through the unicast routing protocol.

For details on how to configure IP addresses of interfaces, see Configuring IP Addresses for Interfaces in the *Quidway S6700 Series Ethernet Switches Configuration Guide - Basic Configurations*. For details on how to configure OSPF, see **OSPF Configuration** in the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP Routing*.

Step 2 Enable multicast on all switches and PIM-SM on all interfaces.

Enable multicast on S6700A and enable PIM-SM on all interfaces. The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not provided here.

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 11
[SwitchA-Vlanif11] pim sm
[SwitchA-Vlanif11] quit
```

Step 3 Enable IGMP on the interfaces connected to hosts.

Enable IGMP on VLANIF 10 on Switch A and configure the IGMP version as IGMPv2. The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not provided here.

NOTE

By default, IGMPv2 is used and you do not need to set the IGMP version here. To use other IGMP versions, run the **igmp version** command to set the version.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp enable
[SwitchA-Vlanif10] igmp version 2
[SwitchA-Vlanif10] quit
```

Step 4 Add VLANIF 10 on Switch A to the multicast group 225.1.1.1 statically. In this manner, the hosts connected to VLANIF 10 can steadily receive the multicast data sent to the multicast group 225.1.1.1.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp static-group 225.1.1.1
```

Step 5 Verify the configuration.

Run the **display igmp interface** command. You can check the configuration and running status of IGMP on each interface. For example, the information about IGMP on VLANIF 10 of Switch A is as follows:

```
[SwitchA] display igmp interface vlanif 10
Vlanif 10(10.110.1.1):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: none
  IGMP limit: -
  Value of query interval for IGMP (negotiated): -
  Value of query interval for IGMP (configured): 60 s
  Value of other querier timeout for IGMP: 0 s
  Value of maximum query response time for IGMP: 10 s
  Querier for IGMP: 10.110.1.1 (this router)
```

Run the **display igmp routing-table** command on Switch A. You can check whether VLANIF 10 is added to the multicast group 225.1.1.1 statically. If the (*, 225.1.1.1) entry exists on Switch

A, the downstream interface is VLANIF 10, and the protocol type is **STATIC**, you can infer that VLANIF 10 is added to the multicast group 225.1.1.1 statically.

```
[SwitchA] display igmp routing-table
Routing table of VPN-Instance: public net
 Total 1 entry
 00001. (*, 225.1.1.1)
     List of 1 downstream interface
     Vlanif10 (10.110.1.1),
     Protocol: STATIC
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10 11
#
 multicast routing-enable
#
interface Vlanif10
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp static-group 225.1.1.1
#
interface Vlanif11
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 11
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 20 21
#
 multicast routing-enable
#
interface Vlanif20
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif21
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 20
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 21
```

```
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 30 31
#
 multicast routing-enable
#
interface Vlanif30
 ip address 10.110.3.2 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif31
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 30
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 31
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

4.4.2 Example for Configuring SSM Mapping

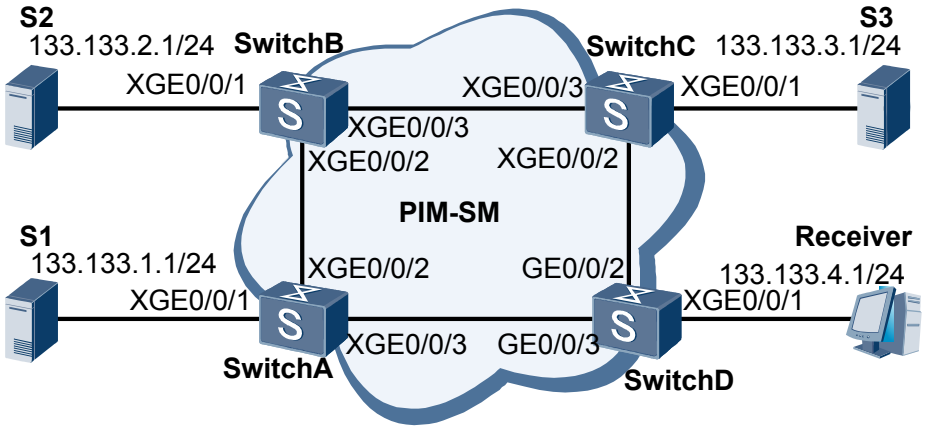
Networking Requirements

On the multicast network as shown in **Figure 4-8**, PIM-SM is run and ASM and SSM models are used to provide multicast services. IGMPv3 is run on the interface on the Switch connected to the Receiver. The IGMP version on the Receiver is IGMPv2 and cannot be upgraded to IGMPv3.

The range of SSM group addresses on the current network is 232.1.1.0/24. S1, S2, and S3 send multicast data to the multicast group whose IP address is in this range. The Receiver receives the multicast data only from S1 and S3.

Solution: Configure SSM mapping on SwitchD.

Figure 4-8 Networking of the SSM mapping configuration



Switch	Physical interfaces	VLANIF interface	IP address
Switch A	XGE0/0/1	VLANIF 10	133.133.1.2/24
	XGE0/0/2	VLANIF 20	192.168.1.1/24
	XGE0/0/3	VLANIF 30	192.168.4.2/24
Switch B	XGE0/0/1	VLANIF 11	133.133.2.2/24
	XGE0/0/2	VLANIF 20	192.168.1.2/24
	XGE0/0/3	VLANIF 31	192.168.2.1/24
Switch C	XGE0/0/1	VLANIF 12	133.133.3.2/24
	XGE0/0/2	VLANIF 21	192.168.3.1/24
	XGE0/0/3	VLANIF 31	192.168.2.2/24
Switch D	XGE0/0/1	VLANIF 13	133.133.4.2/24
	XGE0/0/2	VLANIF 21	192.168.3.2/24
	XGE0/0/3	VLANIF 30	192.168.4.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable SSM mapping on the interfaces of the switches connected to hosts.
2. Set the range of SSM group addresses on all the switches in the PIM-SM domain.
3. Configure the static SSM mapping rules on the switches where SSM mapping is enabled.

Data Preparation

To complete the configuration, you need the following data:

- Range of SSM multicast groups
- IP addresses of Source 1 and Source 3

NOTE

This configuration example describes only the commands used to configure SSM mapping.

Procedure

Step 1 Create VLANs and add interfaces to the VLANs.

Step 2 Configure the IP address of each VLANIF and the unicast routing protocol according to **Figure 4-8**.

Step 3 Enable IGMP and SSM mapping on the interfaces connected to hosts.

```
[SwitchD] multicast routing-enable
[SwitchD] interface vlanif 13
[SwitchD-Vlanif13] igmp enable
[SwitchD-Vlanif13] igmp version 3
[SwitchD-Vlanif13] igmp ssm-mapping enable
[SwitchD-Vlanif13] quit
```

Step 4 Configure the range of SSM group addresses.

Set the range of SSM group addresses to 232.1.1.0/24 on all switches. The configurations of Switch B, SwitchC, and Switch D are similar to configuration of Switch A, and are not provided here.

```
[SwitchA] acl number 2000
[SwitchA-Acl-Basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-Acl-Basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
```

Step 5 Configure static SSM mapping rules on the switches connected to hosts.

Map the multicast group in the range of 232.1.1.0/24 to Source 1 and Source 3.

```
[SwitchD] igmp
[SwitchD-igmp] ssm-mapping 232.1.1.0 24 133.133.1.1
[SwitchD-igmp] ssm-mapping 232.1.1.0 24 133.133.3.1
```

Check the information about SSM mapping of specific sources and group addresses on switches.

```
[SwitchD] display igmp ssm-mapping group
IGMP SSM-Mapping conversion table of VPN-Instance: public net
Total 2 entries
Total 2 entries matched
 00001. (133.133.1.1, 232.1.1.0)
 00002. (133.133.3.1, 232.1.1.0)
```

Step 6 Verify the configuration.

The Receiver joins the group 232.1.1.1.

Run the **display igmp group ssm-mapping** command to view the information about the specific sources or group addresses on the switches. Take the information about the specific source or group address on Switch D for example:

```
[SwitchD] display igmp group ssm-mapping
IGMP SSM mapping interface group report information of VPN-Instance: public net
 Vlanif10 (133.133.4.2):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.1.1.1       133.133.4.1     00:01:44    00:00:26

[SwitchD] display igmp group ssm-mapping verbose
Interface group report information of VPN-Instance: public net
 Vlanif10 (133.133.4.2):
  Total entry on this interface: 1
  Total 1 IGMP SSM-Mapping Group reported
   Group: 232.1.1.1
```

```
    Uptime: 00:01:52
    Expires: 00:00:18
    Last reporter: 133.133.4.1
    Last-member-queryCounter: 0
    Last-member-query-timer-expiry: off
    Group mode: exclude
    Version1-host-present-timer-expiry: off
    Version2-host-present-timer-expiry: 00:00:17
```

Run the **display pim routing-table** command to view the PIM-SM multicast routing table on a switch. Take the information displayed on Switch D for example:

```
[SwitchD] display pim routing-table
VPN-Instance: public net
 Total 2 (S, G) entries
 (133.133.1.1, 232.1.1.1)
     RP: 192.168.3.2
     Protocol: pim-ssm, Flag:EXT NIIF
     UpTime: 00:11:25
     Upstream interface: Vlanif30
         Upstream neighbor: 192.168.4.2
         RPF prime neighbor: 192.168.4.2
     Downstream interface(s) information :
     Total number of downstreams: 1
         1: Vlanif13
             Protocol: igmp, UpTime: 00:11:25, Expires:-

 (133.133.3.1, 232.1.1.1)
     RP: 192.168.3.2
     Protocol: pim-ssm, Flag:EXT NIIF
     UpTime: 00:11:25
     Upstream interface: Vlanif21
         Upstream neighbor: 192.168.3.1
         RPF prime neighbor: 192.168.3.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif13
             Protocol: igmp, UpTime: 00:11:25, Expires:-
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10 20 30
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 133.133.1.2 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 10
```

```
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 133.133.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 11 20 31
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif11
 ip address 133.133.2.2 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 11
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 31
#
ospf 1
 area 0.0.0.0
  network 133.133.2.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 12 21 31
#
 multicast routing-enable
#
acl number 2000
```

```
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif12
 ip address 133.133.3.2 255.255.255.0
 pim sm
#
interface Vlanif21
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 12
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 21
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 31
#
ospf 1
 area 0.0.0.0
  network 133.133.3.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
 vlan batch 13 21 30
#
 multicast routing-enable
#
interface Vlanif13
 ip address 133.133.4.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
#
interface Vlanif21
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 13
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 21
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 133.133.4.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
```

```
  network 192.168.4.0 0.0.0.255
#
pim
 c-Bsr vlanif30
 c-rp vlanif30
 ssm-policy 2000
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
igmp
 ssm-mapping 232.1.1.0 255.255.255.0 133.133.1.1
 ssm-mapping 232.1.1.0 255.255.255.0 133.133.3.1
#
return
```

4.5 PIM-DM (IPv4) Configuration

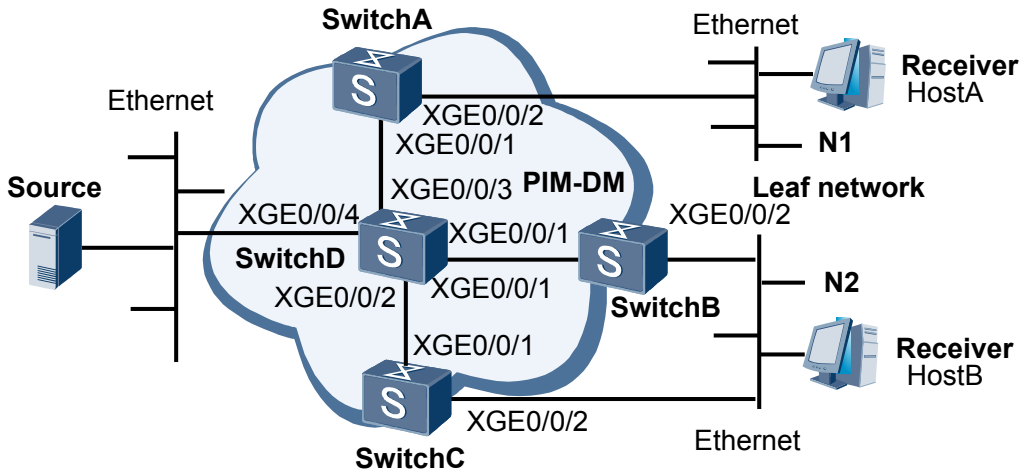
This chapter describes the PIM-DM (IPv4) fundamentals, configuration steps, and maintenance for PIM-DM functions, along with typical examples.

4.5.1 Example for Configuring the PIM-DM Network

Networking Requirements

On the experiment network shown in **Figure 4-9**, multicast is deployed. The unicast routes work normally. The S6700s on the network need to be configured properly so that hosts can receive the VOD information in multicast mode.

Figure 4-9 Networking diagram for configuring basic PIM-DM functions



Switch	Physical interfaces	VLANIF interface	IP address
Switch A	XGE0/0/1	VLANIF100	192.168.1.1/24
	XGE0/0/2	VLANIF101	10.110.1.1/24
Switch B	XGE0/0/1	VLANIF200	192.168.2.1/24

	XGE0/0/2	VLANIF102	10.110.2.1/24
Switch C	XGE0/0/1	VLANIF300	192.168.3.1/24
	XGE0/0/2	VLANIF102	10.110.2.2/24
Switch D	XGE0/0/1	VLANIF200	192.168.2.2/24
	XGE0/0/2	VLANIF300	192.168.3.2/24
	XGE0/0/3	VLANIF100	192.168.1.2/24
	XGE0/0/4	VLANIF103	10.110.5.1/24

Configuration Roadmap

In a small-scale experiment network, PIM-DM is adopted to configure multicast. Enable PIM silent on the VLANIF interfaces of Switch A to protect Switch A from Hello message attacks. The configuration roadmap is as follows:

1. Configure the IP addresses of interfaces and the unicast routing protocol. PIM is an intra-domain multicast routing protocol that depends on a unicast routing protocol. The multicast routing protocol can work normally after the unicast routing protocol works normally.
2. Enable multicast on the switch.
3. Enable PIM-DM on each interface.

Data Preparation

To complete the configuration, you need the following data:

- Address of multicast group G: 225.1.1.1/24
- Address of multicast group S: 10.110.5.100/24
- Version of the IGMP protocol running between routers and hosts: IGMPv2

NOTE

This configuration example describes only the commands used to configure PIM-DM.

Procedure

Step 1 Configure the IP address of each interface and the unicast routing protocol.

Configure IP addresses and masks of interfaces on the switches according to **Figure 4-9**. Configure OSPF between switches to ensure that the switches can communicate at the network layer and update routes through the unicast routing protocol.

For details on how to configure IP addresses of interfaces, see Configuring IP Addresses for Interfaces in the *Quidway S6700 Series Ethernet Switches Configuration Guide - Basic Configuration*. For details on how to configure OSPF, see **3.4 OSPF Configuration** in the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP Routing*.

Step 2 Enable multicast on all switches and enable PIM-DM on all interfaces.

Enable multicast on Switch A and enable PIM-DM on each interface. The configurations of Switch B, Switch C, and Switch D are similar to the configuration of Switch A, and are not provided here.

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 100
```

```
[SwitchA-Vlanif100] pim dm
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim dm
[SwitchA-Vlanif101] quit
```

Step 3 Configure the interfaces connected to hosts to be PIM silent and configure IGMP on the interface.

On Switch A, configure the vlanif interfaces connected to hosts to be PIM silent, and configure IGMP on the interface. The configurations of Switch B, Switch C, and Switch D are similar to configuration of Switch A, and are not provided here.

```
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim silent
[SwitchA-Vlanif101] igmp enable
[SwitchA-Vlanif101] quit
```

Step 4 Verify the configuration.

Run the **display pim interface** command to view the configuration and operating of PIM on the router interface. The display of the PIM configuration on Switch D is as follows:

```
[SwitchD] display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
Vlanif103       up       0         30          1       10.110.5.1(local)
Vlanif100       up       0         30          1       192.168.1.2(local)
Vlanif200       up       1         30          1       192.168.2.2(local)
Vlanif300       up       1         30          1       192.168.3.2(local)
```

Run the **display pim neighbor** command to check the PIM neighbor relationship between the switches. The display of the PIM neighbor relationship on Switch D is as follows:

```
[SwitchD] display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 3

 Neighbor        Interface         Uptime       Expires      Dr-Priority   BFD-
Session
 192.168.1.1     Vlanif100          00:02:22    00:01:27      1
N
 192.168.2.1     Vlanif200          00:00:22    00:01:29      1
N
 192.168.3.1    Vlanif300         00:00:23    00:01:31     1             N
```

Run the **display pim routing-table** command to view the PIM multicast routing table on the switch. Assume that HostA needs to receive the information about multicast group G 225.1.1.1/24. When sending multicast packets to multicast group G, multicast source S 10.110.5.100/24 generates an SPT through flooding and the (S, G) entries exist on Switch A and Switch D that are in the SPT. When HostA joins multicast group G, an (*, G) entry is generated on Switch A. The information displayed on Switch B and Switch C is similar to the information displayed on Switch A. The displayed information is as follows:

```
[SwitchA] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Protocol: pim-dm, Flag: WC
     UpTime: 03:54:19
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif101
             Protocol: igmp, UpTime: 01:38:19, Expires: never
```

```
(10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:00:44
     Upstream interface: Vlanif100
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
          1: Vlanif101
              Protocol: pim-dm, UpTime: 00:00:44, Expires: never

[SwitchD] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: LOC ACT
     UpTime: 01:35:25
     Upstream interface: Vlanif103
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
        1: Vlanif100
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
        2: Vlanif200
            Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 multicast routing-enable
#
vlan batch 100 101
#
interface Vlanif100
 ip address 192.168.1.1 255.255.255.0
 pim dm
#
interface Vlanif101
 ip address 10.110.1.1 255.255.255.0
 pim dm
 pim silent
 igmp enable
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 multicast routing-enable
#
vlan batch 200 102
#
interface Vlanif102
 ip address 10.110.2.1 255.255.255.0
 pim dm
 igmp enable
#
interface Vlanif200
 ip address 192.168.2.1 255.255.255.0
 pim dm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
 multicast routing-enable
#
vlan batch 102 300
#
interface Vlanif102
 ip address 10.110.2.2 255.255.255.0
 pim dm
 igmp enable
#
interface Vlanif300
 ip address 192.168.3.1 255.255.255.0
 pim dm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
#
return
```

- Configuration file of SwitchD

```
#
 sysname SwitchD
#
 multicast routing-enable
#
vlan batch 100 103 200 300
```

```
#
interface Vlanif 100
 ip address 192.168.1.2 255.255.255.0
 pim dm
#
interface Vlanif 103
 ip address 10.110.5.1 255.255.255.0
 pim dm
#
interface Vlanif 200
 ip address 192.168.2.2 255.255.255.0
 pim dm
#
interface Vlanif 300
 ip address 192.168.3.2 255.255.255.0
 pim dm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid tagged vlan 100
#
interface XGigabitEthernet0/0/4
 port hybrid pvid vlan 103
 port hybrid untagged vlan 103
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
#
return
```

4.6 PIM-SM (IPv4) Configuration

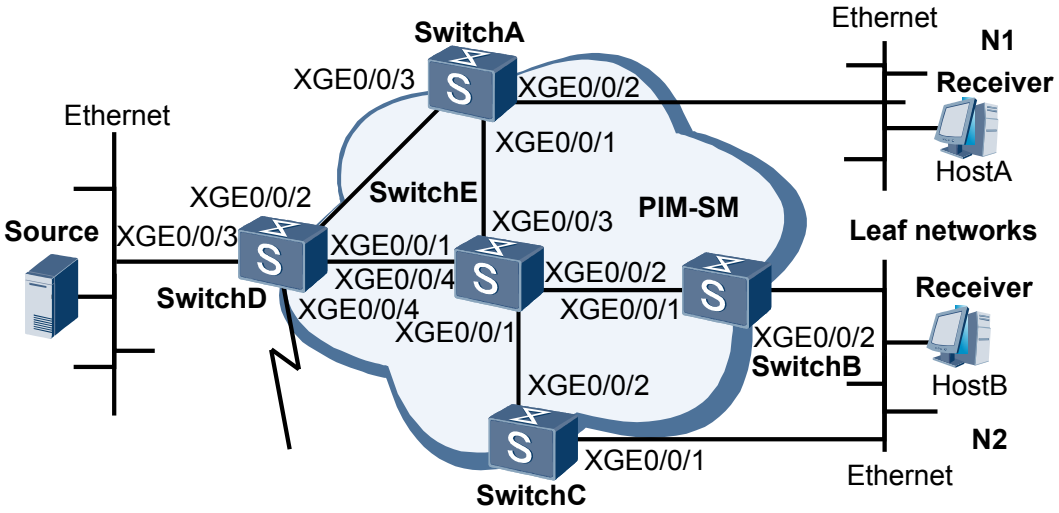
The PIM protocol is used to implement multicast routing and data forwarding inside an AS. The PIM-SM protocol is a multicast routing protocol of sparse node. It is applicable to a large-scale network with sparsely-distributed members.

4.6.1 Example for Configuring the PIM-SM Network

Networking Requirements

As shown in **Figure 4-10**, multicast is deployed on the network of an Internet Service Provider (ISP). The Interior Gateway Protocol (IGP) is deployed on the network. The unicast routing routes work normally and are connected to the Internet. The routers on the network need to be configured properly so that hosts can receive the video on demand (VOD) in multicast mode.

Figure 4-10 Networking diagram for configuring PIM-SM multicast network



Switch	Physical interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF 100	192.168.9.1/24
	XGE 0/0/2	VLANIF 101	10.110.1.1/24
	XGE 0/0/3	VLANIF 200	192.168.1.1/24
Switch B	XGE 0/0/1	VLANIF 300	192.168.2.1/24
	XGE 0/0/2	VLANIF 102	10.110.2.1/24
Switch C	XGE 0/0/1	VLANIF 102	10.110.2.2/24
	XGE 0/0/2	VLANIF 400	192.168.3.1/24
Switch D	XGE 0/0/1	VLANIF 500	192.168.4.2/24
	XGE 0/0/2	VLANIF 200	192.168.1.2/24
	XGE 0/0/3	VLANIF 103	10.110.5.1/24
	XGE 0/0/4	VLANIF 104	10.110.4.1/24
Switch E	XGE 0/0/1	VLANIF 400	192.168.3.2/24
	XGE 0/0/2	VLANIF 300	192.168.2.2/24
	XGE 0/0/3	VLANIF 100	192.168.9.2/24
	XGE 0/0/4	VLANIF 500	192.168.4.1/24

Configuration Roadmap

The ISP network connects to the Internet. The PIM-SM protocol is used to configure the multicast function, which facilitates service expansion. The ASM and SSM models provide multicast services. The configuration roadmap is as follows:

1. Configure the IP addresses of interfaces and the unicast routing protocol. PIM is an intra-domain multicast routing protocol that depends on a unicast routing protocol. The multicast routing protocol can work normally after the unicast routing protocol works normally.
2. Enable multicast on all switches providing multicast services. Before configuring other PIM-SM functions, you must enable the multicast function.
3. Enable PIM-SM on all the interfaces of switches. After PIM-SM is enabled, you can configure other PIM-SM functions.

NOTE

If IGMP is also required on this interface, PIM-SM must be enabled before IGMP is enabled. The configuration order cannot be reversed; otherwise, the configuration of PIM fails.

4. Enable IGMP on the interfaces of switches connected to hosts. A receiver can join and leave a multicast group freely by sending an IGMP message. The leaf switches maintain the multicast membership through IGMP.
5. Enable the PIM silent function on interface that is directly connected to hosts. In this manner, malicious hosts are prevented from simulating PIM Hello messages and security of multicast routers is ensured.

NOTE

PIM silent is applicable only to the interfaces of a switch directly connected to the host network segment that is connected only to this switch.

6. Configure the RP. The RP is a root node of an RPT on the PIM-SM network. It is recommended that you configure the RP on a device that has more multicast flows, for example, Switch E in **Figure 4-10**.

NOTE

- After creating an (*, G) entry according to the new multicast membership, the DR on the user side sends Join/Prune messages towards the RP and updates the shared tree on the path.
- When a multicast data source starts to send data to groups, the DR unicasts the Register message to the RP. After receiving the Register message, the RP decapsulates it and then forwards it to other multicast members along the shared tree. At the same time, the RP sends a Register-Stop message to the DR on the multicast source side. After the Register-Stop is performed, the RPT can be switched to the SPT.

7. (Optional) Set the BSR boundary on the interfaces connected to the Internet. The Bootstrap message cannot pass through the BSR boundary; therefore, the BSR serves only this PIM-SM domain. In this manner, multicast services can be controlled effectively.
8. (Optional) Configure range of SSM group addresses on each Switch . Ensure that switches in the PIM-SM domain provide services only for multicast groups in the range of SSM group addresses. In this manner, multicast can be controlled effectively.

NOTE

This configuration example describes only the commands used to configure PIM-SM.

Data Preparation

To complete the configuration, you need the following data:

- Address of multicast group G: 225.1.1.1/24
- Address of multicast group S: 10.110.5.100/24
- Version of the IGMP protocol running between routers and hosts: IGMPv3
- Range of SSM group addresses: 232.1.1.0/24

Procedure

Step 1 Configure the IP address of each interface and the unicast routing protocol.

Configure IP addresses and masks of interfaces on the switches according to **Figure 4-10**. Configure OSPF between switches to ensure that the switches can communicate at the network layer and update routes through the unicast routing protocol.

For details on how to configure IP addresses of interfaces, see **2.1 IP Addresses Configuration** in the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP*

Service. For details on how to configure OSPF, see **3.4 OSPF Configuration** in the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP Routing*.

Step 2 Enable multicast on all switches and PIM-SM on all interfaces.

Enable multicast on all the switches and enable PIM-SM on all interfaces. The configurations of Switch B, Switch C, and Switch D are similar to the configuration of Switch A, and are not provided here.

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim sm
[SwitchA-Vlanif101] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] pim sm
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] pim sm
[SwitchA-Vlanif200] quit
```

Step 3 Enable IGMP on the interfaces connected to hosts.

Enable IGMP on the interface connecting Switch A to hosts. The configurations of Switch B, Switch C, and Switch D are similar to configuration of Switch A, and are not provided here.

```
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] igmp enable
[SwitchA-Vlanif101] igmp version 3
```

Step 4 Enable PIM silent on Switch A.

```
[SwitchA] interface vlanif 101
[SwitchA-Vlanif101] pim silent
```

Step 5 Configure the RP.

NOTE

The RP can be configured in two modes: the static RP and the dynamic RP. The static RP can be configured together with the dynamic RP. You can also configure only the static RP or the dynamic RP. When the static RP and the dynamic RP are configured simultaneously, you can change the parameter values to specify which RP is preferred.

This example shows how to configure the static RP and the dynamic RP and to specify the dynamic RP as the preferred RP and the static RP as the standby RP.

Configure the dynamic RP on one or more switches in the PIM-SM domain. In this example, set the service range of the RP and specify the locations of the C-BSR and the C-RP on Switch E.

```
[SwitchE] acl number 2008
[SwitchE-acl-basic-2008] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2008] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlanif 100
[SwitchE-pim] c-rp vlanif 100 group-policy 2008 priority 0
```

Configure static RPs on all switches. The configurations of Switch B, Switch C, Switch D, and Switch E are similar to configuration on Switch A, and are not provided here.

NOTE

If you enter **preferred** to the right of **static-rp** *X.X.X.X*, the static RP is selected as the RP in the PIM-SM domain.

```
[SwitchA] pim
[SwitchA-pim] static-rp 192.168.2.2
```

Step 6 Configure the BSR boundary on the interface connecting Switch D to the Internet.

```
[SwitchD] interface vlanif 104
[SwitchD-Vlanif104] pim bsr-boundary
[SwitchD-Vlanif104] quit
```

Step 7 Configure the range of SSM group addresses.

Set the range of SSM group addresses to 232.1.1.0/24 on all switches. The configurations of Switch B, Switch C, Switch D, and Switch E are the same as the configuration of Switch A, and are not provided here.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
```

Step 8 Verify the configuration.

Run the **display pim interface** command. You can view the configuration and running status of PIM on the interface. For example, the PIM information displayed on Switch C is as follows:

```
[SwitchC] display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
Vlanif102        up      0         30         1         10.110.2.2    (local)
Vlanif400        up      1         30         1         192.168.3.1
```

Run the **display pim bsr-info** command to view information about BSR election on the switches. For example, the BSR information on Switch A and Switch E (including the C-BSR information on Switch E) is as follows:

```
[SwitchA] display pim bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 192.168.9.2
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 01:40:40
     Expires: 00:01:42
     C-RP Count: 1

[SwitchE] display pim bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 192.168.9.2
     Priority: 0
     Mask length: 30
     State: Elected
     Scope: Not scoped
     Uptime: 00:00:18
     Next BSR message scheduled at :00:01:42
     C-RP Count: 1
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address is: 192.168.9.2
     Priority: 0
     Hash mask length: 30
     State:Elected
     Scope: Not scoped
     Wait to be BSR: 0
```

Run the **display pim rp-info** command to view the RP information on the switches. For example, the RP information displayed on Switch A is as follows:

```
[SwitchA] display pim rp-info
VPN-Instance: public net
```

```
 PIM-SM BSR RP information:
 Group/MaskLen: 225.1.1.0/24
     RP: 192.168.9.2
     Priority: 0
     Uptime: 00:45:13
     Expires: 00:02:17
 PIM SM static RP information:
     Static RP: 192.168.2.2
```

Run the **display pim routing-table** command. You can view the PIM multicast routing table. Host A needs to receive the information from group 225.1.1.1/24, and HostB needs to receive the information sent by the source 10.110.5.100/24 to the group 232.1.1.1/24. The displayed information is as follows:

```
[SwitchA] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 192.168.9.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:46
     Upstream interface:  Vlanif 100,
         Upstream neighbor: 192.168.9.2
         RPF neighbor: 192.168.9.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif 101
             Protocol: igmp, UpTime: 00:13:46, Expires:-

(10.110.5.100, 225.1.1.1)
     RP: 192.168.9.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:00:42
     Upstream interface: Vlanif 200
         Upstream neighbor: 192.168.1.2
         RPF neighbor: 192.168.1.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif101
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-

[SwitchD] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 2 (S, G) entry

 (10.110.5.100, 225.1.1.1)
     RP: 192.168.9.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:00:42
     Upstream interface: vlanif103
         Upstream neighbor: 10.110.5.100
         RPF neighbor: 10.110.5.100
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif200
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-

(10.110.5.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:20
     Upstream interface: vlanif103
         Upstream neighbor: 10.110.5.100
         RPF neighbor: 10.110.5.100
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif500
             Protocol: pim-ssm, UpTime: 00:01:20, Expires:-
```

```
[SwitchE] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     RP: 192.168.9.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:16
     Upstream interface: Register
         Upstream neighbor: 192.168.4.2
         RPF neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif100
             Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22

(10.110.5.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:22
     Upstream interface: vlanif500
         Upstream neighbor: 192.168.4.2
         RPF neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif400
             Protocol: pim-ssm, UpTime: 00:01:22, Expires:-

[SwitchC] display pim routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (10.110.5.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:25
     Upstream interface: vlanif400
         Upstream neighbor: 192.168.3.2
         RPF neighbor: 192.168.3.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif102
             Protocol: igmp, UpTime: 00:01:25, Expires:-
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 100 101 200
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif100
 ip address 192.168.9.1 255.255.255.0
 pim sm
#
interface Vlanif101
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 pim silent
#
```

```
interface Vlanif200
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.9.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 multicast routing-enable
#
vlan batch 102 300
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif 102
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface Vlanif300
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 102 400
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif102
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface Vlanif400
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
 vlan batch 103 104 200 500
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif103
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
interface Vlanif104
 ip address 10.110.4.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface Vlanif200
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif500
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
```

```
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 103
 port hybrid untagged vlan 103
#
interface XGigabitEthernet0/0/4
 port hybrid pvid vlan 104
 port hybrid untagged vlan 104
#
ospf 1
 area 0.0.0.0
  network 10.110.4.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

- Configuration file of Switch E

```
#
 sysname SwitchE
#
 vlan batch 100 300 400 500
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
acl number 2008
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface Vlanif100
 ip address 192.168.9.2 255.255.255.0
 pim sm
#
interface Vlanif300
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlanif400
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif500
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/4
 port hybrid pvid vlan 500
```

```
 port hybrid untagged vlan 500
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.9.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 c-bsr vlanif 100
 c-rp vlanif 100 group-policy 2008 priority 0
 static-rp 192.168.2.2
 ssm-policy 2000
#
return
```

4.6.2 Example for Configuring PIM BFD

Networking Requirements

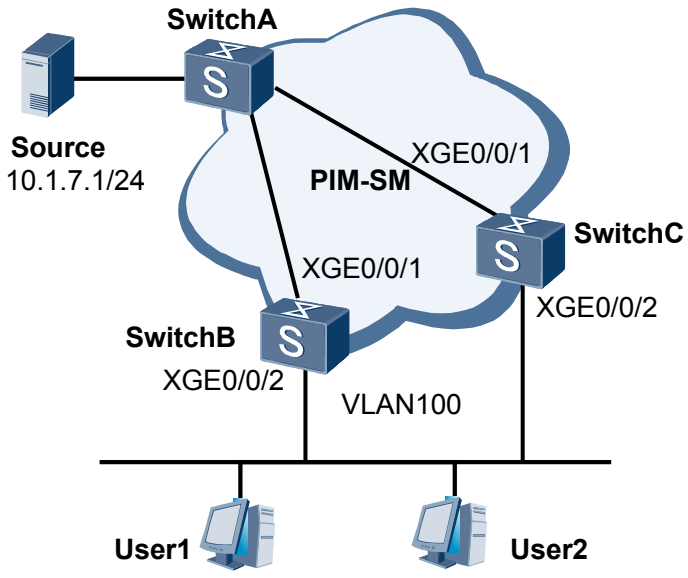
On the multicast network shown in **Figure 4-11**, PIM-SM is run between switches. Hosts receive the VOD information from the multicast source. Switch A is the DR on the source side. Switch B and Switch C are connected to the segment where hosts reside. When the DR changes, other switches on the network segment can detect the change of the DR quickly.

You can set up the BFD session on the network segment where the host is located to respond to the changes of the DR quickly. In addition, you can configure the DR switchover delay. In this case, when a switch is added to the network segment and may become a DR, the multicast routing table of the original DR is reserved until the routing entries of the new DR are created. Therefore, the packet loss due to the delay in creating multicast entries is prevented.

NOTE

After the delay of PIM DR switchover is set, the downstream receiver may receive two copies of the same data during the DR switchover and the assert mechanism will be triggered. If you do not want to trigger the assert mechanism, you do not need to set the DR switchover delay.

Figure 4-11 Configuring the PIM BFD networking in the shared network segment



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure PIM BFD on the interfaces that connect switches to the network segment where the host is located.
2. Set the PIM DR switchover delay on the interfaces that connect switches to the network segment where the host is located.

Data Preparation

To complete the configuration, you need the following data:

- Parameters of PIM BFD sessions
- PIM DR switchover delay

NOTE

This configuration example describes only the commands used to configure PIM-SM BFD.

Procedure

Step 1 Configure the IP address of each interface and the unicast routing protocol.

Configure IP addresses and masks of interfaces on the switches according to **Figure 4-11**. Configure OSPF between switches to ensure that the switches can communicate at the network layer and update routes through the unicast routing protocol.

For details on how to configure IP addresses of interfaces, see **2.1 IP Addresses Configuration** in the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP Service*. For details on how to configure OSPF, see **3.4 OSPF Configuration** in the *Quidway S6700 Series Ethernet Switches Configuration Guide - IP Routing*.

Step 2 Enable BFD globally and configure PIM BFD in the interface view.

Enable BFD globally on Switch B and Switch C, enable PIM BFD on the interfaces that are connected to the network segment where the host resides, and set PIM BFD parameters. The configuration on Switch C is similar to the configuration on Switch B and is not provided here.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] pim bfd enable
[SwitchB-Vlanif100] pim bfd min-tx-interval 200 min-rx-interval 200 detect-
multiplier 3
```

Step 3 Configure the PIM DR switchover delay.

Configure PIM DR switchover delay on Switch B and SwitchC. The configuration on SwitchC is similar to the configuration on SwitchB and is not provided here.

```
[SwitchB-Vlanif100] pim timer dr-switch-delay 20
[SwitchB-Vlanif100] quit
[SwitchB] quit
```

Step 4 Verify the configuration.

Run the **display pim interface verbose** command, and you can view detailed information about the interface that runs PIM. The information about the interface that runs PIM on Switch

B indicates that the DR on the network segment where the host is located is Switch C. PIM BFD is enabled on the interface and the switchover delay is set.

```
[SwitchB] display pim interface vlanif100 verbose
VPN-Instance: public net
 Interface: Vlanif100, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM Hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM Hello override interval (negotiated): 2500 ms
     PIM Hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0XF5712241
     PIM Hello hold interval: 105 s
     PIM Hello assert interval: 180 s
     PIM triggered Hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: enable
     PIM BFD min-tx-interval: 200 ms
     PIM BFD min-rx-interval: 200 ms
     PIM BFD detect-multiplier: 3
     PIM dr-switch-delay timer : 20 s
     Number of routers on network not using DR priority: 0
     Number of routers on network not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 2
```

Run the **display pim bfd session** command to display information about the BFD session on each switch. You can check whether the BFD session is set up on each switch.

```
[SwitchB] display pim  bfd session
VPN-Instance: public net
Total 1 BFD session Created

Vlanif100 (10.1.1.1): Total 1 BFD session Created

Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
10.1.1.2     200           200           3            8192/8192        Up
```

Run the **display pim routing-table** command to view the PLM routing table. SwitchC functions as the DR. The (S, G) and (*, G) entries exist. The displayed information is as follows:

```
[SwitchC] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 10.1.5.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:46
     Upstream interface:     vlanif200,
         Upstream neighbor: 10.1.2.2
         RPF neighbor: 10.1.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif100,
             Protocol: igmp, UpTime: 00:13:46, Expires:-
(10.1.7.1, 225.1.1.1)
     RP: 10.1.5.2
     Protocol: pim-sm, Flag: SPT ACT
```

```
    UpTime: 00:00:42
    Upstream interface: vlanif200
        Upstream neighbor: 10.1.2.2
        RPF neighbor: 10.1.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif100
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

----End

Configuration Files

- SwitchA needs to be configured with only basic PIM SM functions. The configuration file is not provided here.
- The following is the configuration file of Switch B. The configuration file of Switch C is similar to the configuration file of Switch B, and is not provided here.

```
#
 sysname SwitchB
#
 vlan batch 100 200
#
 multicast routing-enable
#
bfd
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 pim sm
 igmp enable
 pim bfd enable
 pim bfd min-tx-interval 200 min-rx-interval 200 detect-multiplier 3
 pim timer dr-switch-delay 20
#
interface Vlanif200
 ip address 10.1.2.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 200
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
return
```

4.7 MSDP Configuration

The MSDP protocol is used to implement multicast routing and data forwarding between PIM-SM domains and anycast RP in a PIM-SM domain.

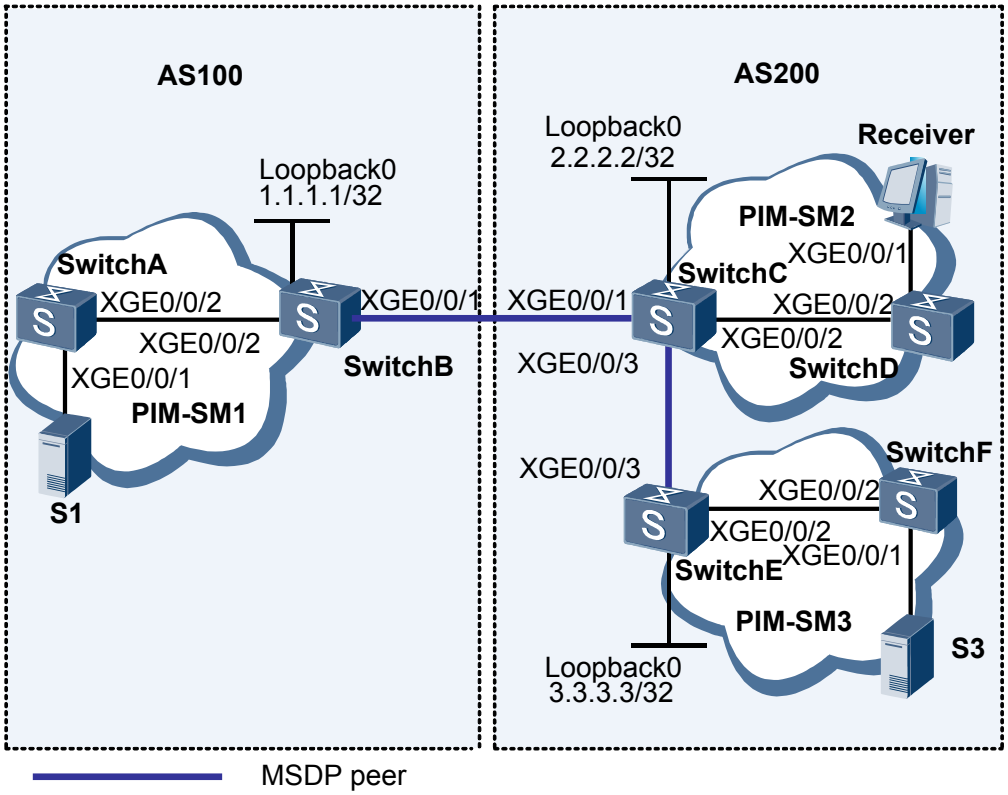
4.7.1 Example for Configuring Basic MSDP Functions

Networking Requirements

As shown in **Figure 4-12**, two ASs exist on the network. Each AS contains one or more PIM-SM domains; each PIM-SM domain has 0 or 1 multicast source and receiver. The receivers in

PIM-SM2 need to receive the multicast data sent by S3 in the PIM-SM3 domain and multicast data sent by S1 in the PIM-SM1 domain.

Figure 4-12 Networking diagram for configuring basic MSDP functions



Switch	Physical interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF 101	10.110.1.1/24
	XGE 0/0/2	VLANIF 100	192.168.1.1/24
Switch B	XGE 0/0/1	VLANIF 200	192.168.2.1/24
	XGE 0/0/2	VLANIF 100	192.168.1.2/24
Switch C	XGE 0/0/1	VLANIF 200	192.168.2.2/24
	XGE 0/0/2	VLANIF 300	192.168.3.1/24
	XGE 0/0/3	VLANIF 400	192.168.4.1/24
Switch D	XGE 0/0/1	VLANIF 102	10.110.2.1/24
	XGE 0/0/2	VLANIF 300	192.168.3.2/24
Switch E	XGE 0/0/2	VLANIF 500	192.168.5.1/24
	XGE 0/0/3	VLANIF 400	192.168.4.2/24
Switch F	XGE 0/0/1	VLANIF 103	10.110.3.1/24
	XGE 0/0/2	VLANIF 500	192.168.5.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP addresses of the interfaces on each switch and configure OSPF in the AS to ensure that the unicast routes within the AS are reachable.

2. Configure EBGP peers and import BGP and OSPF routes into each other's routing table to ensure that the unicast routes between ASs are reachable.
3. Enable multicast and PIM-SM on each interface, configure the boundary domain, and enable the IGMP function on the interfaces connected to hosts.
4. Configure the CBSR and C-RP. Configure the RPs of PIM-SM1 and PIM-SM2 on the ASBR.
5. Establish MSDP peer relationship between RPs of each domain. The MSDP peers and the EBGP peers between ASs use the same interface addresses. According to the RPF rule, the switches receive SA messages from the next hop toward the source RP.

Data Preparation

To complete the configuration, you need the following data:

- Address of multicast group G: 225.1.1.1/24
- Number of the AS that Switch A and Switch B belong to, namely 100, and router ID of Switch B, namely, 1.1.1.1
- Number of the AS that Switch C and Switch D belong to, namely 200, and Router ID of Switch C, namely, 2.2.2.2
- Number of the AS that Switch E and Switch F belong to, namely 200

NOTE

This configuration example describes only the commands related to MSDP configuration.

Procedure

Step 1 Configure the IP addresses of interfaces and the unicast routing protocol.

According to **Figure 4-12**, configure IP addresses and masks for the interfaces on each switch. Configure the OSPF protocol between switches. Ensure the communication on the network layer within an AS. Ensure the dynamic route update between switches through unicast routing protocol. The configuration procedure is not provided here.

Step 2 Configure EBGP peer relationship between ASs and import routes of BGP and OSPF into each other's routing table.

Configure EBGP on Switch B and import OSPF routes.

```
[SwitchB] bgp 100
[SwitchB-bgp] router-id 1.1.1.1
[SwitchB-bgp] peer 192.168.2.2 as-number 200
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

Configure EBGP on Switch C and import OSPF routes.

```
[SwitchC] bgp 200
[SwitchC-bgp] router-id 2.2.2.2
[SwitchC-bgp] peer 192.168.2.1 as-number 100
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] quit
```

Import BGP routes to OSPF on Switch B. The configuration on Switch C is similar to the configuration on Switch B, and is not provided here.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

Step 3 Enable multicast, enable PIM-SM on all interfaces, configure the domain boundary, and enable IGMP on the interface connecting to the host.

Enable multicast on Switch B and enable PIM-SM on each interface. The configurations of other switches are similar to the configuration of Switch B, and are not provided here.

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] pim sm
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif200] pim sm
```

Configure the domain boundary on VLANIF 100 of Switch B.

```
[SwitchB-Vlanif100] pim bsr-boundary
[SwitchB-Vlanif100] quit
```

Configure the domain boundary on VLANIF 200 and VLANIF 400 of Switch C. Configure the service boundary of BSR on VLANIF 400 of Switch E. The configuration on Switch E is similar to the configuration on Switch B, and is not provided here.

Enable IGMP on the interface connecting Switch D to the leaf network.

```
[SwitchD] interface vlanif 102
[SwitchD-Vlanif102] igmp enable
```

Step 4 Configure the CBSR and C-RP.

Create Loopback0, and then configure a CBSR, and a C-RP on Loopback0 on Switch B. The configurations of Switch C and Switch E are similar to the configuration of Switch B, and are not provided here.

```
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] ip address 1.1.1.1 255.255.255.255
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] pim
[SwitchB-pim] cBsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

Step 5 Configure MSDP peer relations.

Configure the MSDP peer relationship on Switch B.

```
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.2.2 connect-interface vlanif200
[SwitchB-msdp] quit
```

Configure the MSDP peer relationship on Switch C.

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.2.1 connect-interface vlanif200
[SwitchC-msdp] peer 192.168.4.2 connect-interface vlanif400
[SwitchC-msdp] quit
```

Configure the MSDP peer relationship on Switch E.

```
[SwitchE] msdp
[SwitchE-msdp] peer 192.168.4.1 connect-interface vlanif400
[SwitchE-msdp] quit
```

Step 6 Verify the configuration.

Run the **display bgp peer** command to view the BGP peer relationship between switches. For example, the following information shows the BGP peer relationship on Switch B and Switch C:

```
[SwitchB] display bgp peer

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Total number of peers : 1                    Peers in established state : 1

  Peer          V   AS   MsgRcvd    MsgSent    OutQ    Up/Down    State
PrefRcv

  192.168.2.2   4   200   24         21          0      00:13:09   Established   6

[SwitchC] display bgp peer

BGP local router ID : 2.2.2.2
 Local AS number : 200
 Total number of peers : 1                    Peers in established state : 1

  Peer          V   AS    MsgRcvd    MsgSent     OutQ   Up/Down    State
PrefRcv

  192.168.2.1   4   100   18         16          0      00:12:04   Established   1
```

Run the **display bgp routing-table** command to view the BGP routing table on a switch. For example, the BGP routing table displayed on Switch C is as follows:

```
[SwitchC] display bgp routing-table

 Total Number of Routes: 5
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            NextHop         MED        LocPrf    PrefVal Path/Ogn
 *>    1.1.1.1/32         192.168.2.1     0                    0       100?
 *>i   2.2.2.2/32         0.0.0.0         0                    0       ?
 *>    192.168.2.0        0.0.0.0         0                    0       ?
 *>    192.168.2.1/32     0.0.0.0         0                    0       ?
 *>    192.168.2.2/32     0.0.0.0         0                    0       ?
```

Run the **display msdp brief** command to view the status of the MSDP peer relationship between switches. The information about establishing MSDP peer relationship among Switch B, Switch C and Switch E is as follows:

```
[SwitchB] display msdp brief

MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.2.2        UP        00:12:27        200    13         0

[SwitchC] display msdp brief

MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  2            2            0            0            0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.2.1        UP        01:07:08        100    8          0
  192.168.4.2        UP        00:06:39        200    13         0
```

```
[SwitchE] display msdp brief

MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0
  Peer's Address     State     Up/Down time    AS     SA Count    Reset Count
  192.168.4.1        UP        00:15:32        200    8           0
```

Run the **display msdp peer-status** command to view the details about MSDP peer relations between switches. The details displayed on Switch B are as follows:

```
[SwitchB] display msdp peer-status

  MSDP Peer 192.168.2.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:15:47
    Resets: 0
    Connection interface: vlanif200 (192.168.2.1)
    Number of sent/received messages: 16/16
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:17:51
  Information about (Source, Group)Based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SACache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
    Peer authentication: unconfigured
    Peer authentication type: none
```

Run the **display pim routing-table** command to view the PIM routing table on a switch. When multicast sources S1 (10.110.1.2/24) in PIM-SM1 and S3 (10.110.3.2/24) in PIM-SM3 send multicast data to multicast group G (225.1.1.1/24), Receiver (10.110.2.2/24) in PIM-SM2 can receive the multicast data. The PIM routing tables displayed on Switch B and Switch C are as follows:

```
[SwitchB] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.1.2, 225.1.1.1)
     RP: 1.1.1.1(local)
     Protocol: pim-sm, Flag: SPT EXT ACT
     UpTime: 00:00:42
     Upstream interface: vlanif200
         Upstream neighbor: 192.168.1.1
         RPF neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif100
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-

[SwitchC] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 2 (S, G) entries

(*, 225.1.1.1)
```

```
     RP: 2.2.2.2(local)
     Protocol: pim-sm, Flag: WC RPT
     UpTime: 00:13:46
     Upstream interface: NULL,
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif300,
             Protocol: pim-sm, UpTime: 00:13:46, Expires:-
(10.110.1.2, 225.1.1.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT MSDP ACT
     UpTime: 00:00:42
     Upstream interface: vlanif200
         Upstream neighbor: 192.168.2.1
         RPF neighbor: 192.168.2.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif300
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-
(10.110.3.2, 225.1.1.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT MSDP ACT
     UpTime: 00:00:42
     Upstream interface: vlanif400
         Upstream neighbor: 192.168.4.2
         RPF neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: vlanif300
             Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 100 101
#
 multicast routing-enable
#
interface Vlanif100
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlanif101
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 100 200
#
 multicast routing-enable
#
interface Vlanif100
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif200
 ip address 192.168.2.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
bgp 100
 router-id 1.1.1.1
 peer 192.168.2.2 as-number 200
 import-route ospf 1
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.2.2 connect-interface vlanif200
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
 multicast routing-enable
#
interface Vlanif200
 ip address 192.168.2.2 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface Vlanif300
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlanif400
 ip address 192.168.4.1 255.255.255.0
 pim sm
```

```
 pim bsr-boundary
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
bgp 200
 router-id 2.2.2.2
 peer 192.168.2.1 as-number 100
 import-route ospf 1
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.2.1 connect-interface vlanif200
 peer 192.168.4.2 connect-interface vlanif400
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
 vlan batch 102 300
#
 multicast routing-enable
#
interface Vlanif102
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif300
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
```

```
#
return
```

- Configuration file of Switch E

```
#
 sysname SwitchE
#
 vlan batch 400 500
#
 multicast routing-enable
#
interface Vlanif 400
 ip address 192.168.4.2 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface Vlanif 500
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.4.1 connect-interface vlanif400
#
return
```

- Configuration file of Switch F

```
#
 sysname SwitchF
#
 vlan batch 103 500
#
 multicast routing-enable
#
interface Vlanif103
 ip address 10.110.3.1 255.255.255.0
 pim sm
#
interface Vlanif500
 ip address 192.168.5.2 255.255.255.0
 pim sm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 103
 port hybrid untagged vlan 103
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 500
 port hybrid untagged vlan 500
```

```
#
ospf 1
 area 0.0.0.0
  network 192.168.5.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
#
return
```

4.8 IPv4 Multicast Routing Management

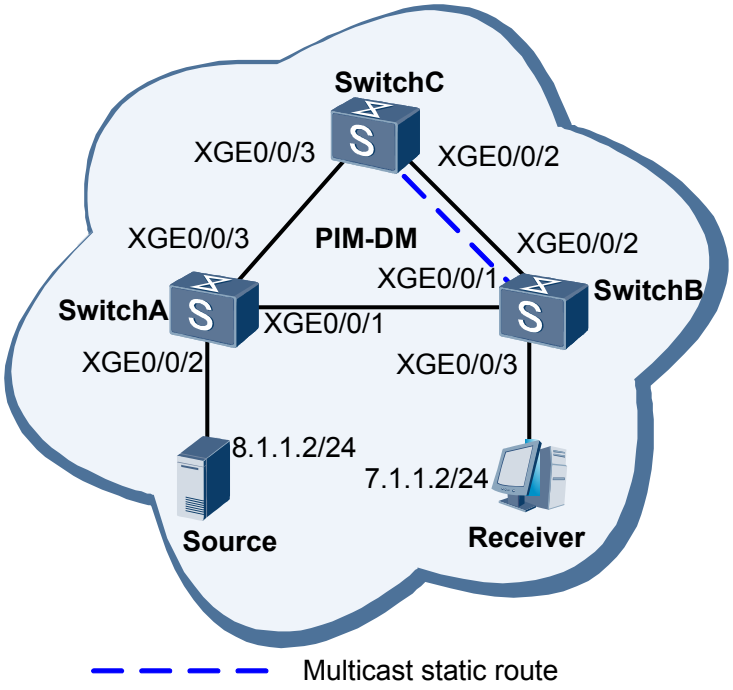
The system synchronously maintains multiple multicast routing protocols, and controls multicast routing and forwarding through the information exchanged between the control plane and the forwarding plane.

4.8.1 Example for Changing Static Multicast Routes to RPF Routes

Networking Requirements

As shown in **Figure 4-13**, PIM-DM runs on the network and all the switches support multicast. The receiver can receive information from the multicast source. Switch A, Switch B, and Switch C run OSPF. You need to configure a static multicast route to make the multicast path from the source to the receiver different from the unicast path from the source to the receiver.

Figure 4-13 Networking diagram for changing static multicast routes to RPF routes



Switch	Physical interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF 10	9.1.1.1/24
	XGE 0/0/2	VLANIF 20	8.1.1.1/24
	XGE 0/0/3	VLANIF 30	12.1.1.1/24
Switch B	XGE 0/0/1	VLANIF 10	9.1.1.2/24
	XGE 0/0/2	VLANIF 40	13.1.1.1/24

	XGE 0/0/3	VLANIF 50	7.1.1.1/24
Switch C	XGE 0/0/2	VLANIF 40	13.1.1.2/24
	XGE 0/0/3	VLANIF 30	12.1.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP addresses of interfaces and the unicast routing protocol on each switch.
2. Enable the multicast function on all switches, PIM-SM on all interfaces, and IGMP on the interfaces at the host side.
3. Configure static multicast RPF routes on Switch B, and configure Switch C as the RPF neighbor.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the source
- Outgoing interface of the route from Switch B to SwitchC: VLANIF 40

NOTE

This configuration example describes only the commands used to configure static multicast routes.

Procedure

Step 1 Configure the IP addresses of interfaces and the unicast routing protocol on each switch.

Configure the IP addresses and masks on the interfaces on each switch according to **Figure 4-13**. IP addresses must be configured on the VLANIF interfaces. OSPF runs between Switch A, Switch B and Switch C, and the switches can update routes among them through the unicast routing protocol. The configuration procedure is not provided here.

Step 2 Enable multicast on all switches and PIM-DM on all interfaces.

Enable multicast on all switches, and PIM-SM on all interfaces. Enable the IGMP function on the interfaces at the host side. The configurations of other switches are similar to configuration of Switch B, and are not provided here.

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] pim dm
[SwitchB-Vlanif10] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] pim dm
[SwitchB-Vlanif40] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] pim dm
[SwitchB-Vlanif50] igmp enable
[SwitchB-Vlanif50] quit
```

Run the **display multicast rpf-info** command on Switch B to view the RPF information of the source. The RPF routes are unicast routes, and the RPF neighbor is Switch A. The following information is displayed:

```
[SwitchB] display multicast rpf-info 8.1.1.2
VPN-Instance: public net
RPF information about source 8.1.1.2:
     RPF interface: vlanif10, RPF neighbor: 9.1.1.1
     Referenced route/mask: 8.1.1.0/24
     Referenced route type: unicast
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Step 3 Configure the static multicast route.

Configure a static multicast RPF route on Switch B, and configure Switch C as the RPF neighbor.

```
[SwitchB] ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
```

Step 4 Verify the configuration.

Run the **display multicast rpf-info** command on Switch B to view the RPF information of the source. The RPF information is as follows. The RPF routes and the RPF neighbor are updated according to the static multicast route.

```
[SwitchB] display multicast rpf-info 8.1.1.2
VPN-Instance: public net
RPF information about source 8.1.1.2:
     RPF interface: vlanif40, RPF neighbor: 13.1.1.2
     Referenced route/mask: 8.1.1.0/24
     Referenced route type: mstatic
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10 20 30
#
 multicast routing-enable
#
interface Vlanif10
 ip address 9.1.1.1 255.255.255.0
 pim dm
#
interface Vlanif20
 ip address 8.1.1.1 255.255.255.0
 pim dm
#
interface Vlanif30
 ip address 12.1.1.1 255.255.255.0
 pim dm
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
```

```
ospf 1
 area 0.0.0.0
  network 8.1.1.0 0.0.0.255
  network 9.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10 40 50
#
 multicast routing-enable
#
interface Vlanif10
 ip address 9.1.1.2 255.255.255.0
 pim dm
#
interface Vlanif40
 ip address 13.1.1.1 255.255.255.0
 pim dm
#
interface Vlanif50
 ip address 7.1.1.1 255.255.255.0
 pim dm
 igmp enable
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
ospf 1
 area 0.0.0.0
  network 7.1.1.0 0.0.0.255
  network 9.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
ip rpf-route-static 8.1.1.0 255.255.255.0 13.1.1.2
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 30 40
#
 multicast routing-enable
#
interface Vlanif30
 ip address 12.1.1.2 255.255.255.0
 pim dm
#
interface Vlanif40
 ip address 13.1.1.2 255.255.255.0
 pim dm
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
```

```
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
return
```

4.9 MLD Snooping Configuration

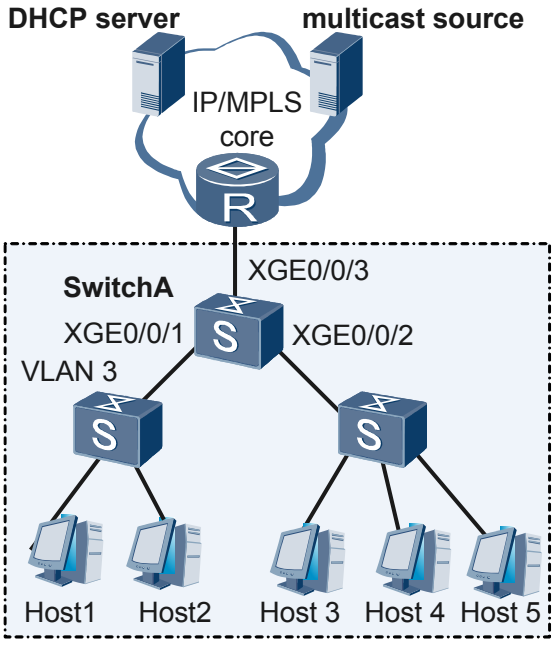
This chapter describes the implementation and configuration procedures of Multicast Listener Discovery (MLD) snooping on the S6700.

4.9.1 Example for Configuring Prompt Leave of Interfaces in a VLAN

Networking Requirements

As shown in **Figure 4-14**, XGE 0/0/1 and XGE 0/0/2 on of Switch A are connected to only one receiver respectively. Other hosts connected to XGE 0/0/1 and XGE 0/0/2 do not need to receive multicast packets. Therefore, when receiving MLD Leave messages from the two interfaces, Switch A deletes the forwarding entries of the multicast groups that the hosts leave without waiting for the timeout of the aging timer. This saves the bandwidth and system resources.

Figure 4-14 Networking diagram for configuring prompt leave of interfaces in a VLAN



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 3 on Switch A and add XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 to VLAN 3.
2. Enable MLD snooping globally on Switch A.
3. Enable prompt leave of interfaces in VLAN 3 on Switch A.
4. Enable MLD snooping in VLAN 3 on Switch A.

Data Preparation

To complete the configuration, you need the following data:

- ID of the VLAN where prompt leave is enabled: 3

Procedure

Step 1 Create VLAN 3 on Switch A and add XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 to VLAN 3. The configuration procedure is not provided here.

Step 2 Enable MLD snooping globally on Switch A.

```
[SwitchA] mld-snooping enable
```

Step 3 Enable prompt leave of interfaces in VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] mld-snooping prompt-leave
```

Step 4 Enable MLD snooping in VLAN 3.

```
[SwitchA-vlan3] mld-snooping enable
```

Step 5 Verify the configuration. Run the **display mld-snooping** command on Switch A.

```
[SwitchA] display mld-snooping vlan 3
 MLD Snooping Vlan Information for VLAN 3
     MLD Snooping is Enable
     MLD Version is Set to default 1
     MLD Query Interval is Set to default 125
     MLD Max Response Interval is Set to default 10
     MLD Robustness is Set to default 2
     MLD Last Member Query Interval is Set to default 1
     MLD Router Port Aging Interval is Set to 180s or holdtime in hello
     MLD Filter Group-Policy is Set to default : Permit All
     MLD Prompt Leave Enable
     MLD Router Alert is Not Required
     MLD Send Router Alert Enable
     MLD Snooping Querier Disable
```

As shown in the preceding output, "MLD Prompt Leave enable" indicates that the configuration of prompt leave for interfaces in VLAN 3 is successful.

----End

Configuration Files

```
#
 sysname SwitchA
#
 mld-snooping enable
#
 vlan batch 3
#
```

```
vlan 3
 mld-snooping enable
 mld-snooping prompt-leave
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 3
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 3
#
interface XGigabitEthernet0/0/3
 port hybrid tagged vlan 3
#
return
```

5 Configuration Guide - QoS

About This Chapter

This document describes QoS features of the S6700 including class-based QoS, traffic policing, traffic shaping, congestion avoidance, and congestion management from function introduction, configuration methods, maintenance and configuration examples. This document guides you through the configuration and the applicable environment of QoS.

5.1 Class-based QoS Configuration
This chapter describes the basic concepts of the traffic classifier, traffic behavior, traffic policy, and priority mapping, and configuration methods and configuration examples of the traffic policy based on complex traffic classification and priority mapping based on simple traffic classification.

5.2 Traffic Policing and Traffic Shaping Configuration
This document describes basic concepts of traffic policing and traffic shaping, and introduces the configuration method of traffic policing based on a traffic classifier, and traffic shaping, and provides configuration examples.

5.3 Congestion Avoidance and Congestion Management Configuration
This chapter describes the basic concepts of congestion avoidance and congestion management, and provides configuration methods and configuration examples of congestion avoidance and congestion management.

5.1 Class-based QoS Configuration

This chapter describes the basic concepts of the traffic classifier, traffic behavior, traffic policy, and priority mapping, and configuration methods and configuration examples of the traffic policy based on complex traffic classification and priority mapping based on simple traffic classification.

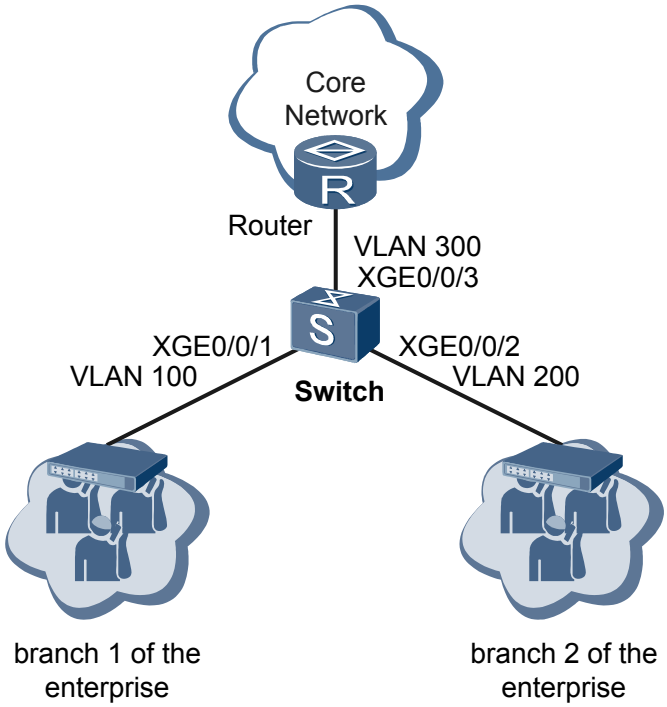
5.1.1 Example for Configuring Priority Mapping Based on Simple Traffic Classification

After priority mapping based on simple traffic classification is configured, the S6700 maps 802.1p priorities of packets to different CoS to provide differentiated services.

Networking Requirements

As shown in **Figure 5-1**, the Switch is connected to the router through XGE 0/0/3; branch 1 and branch 2 of the enterprise access the network through the Switch and router. Branch 1 and branch 2 of the enterprise belong to VLANs 100 and 200. Branch 1 requires better QoS guarantee; therefore, the priority of data packets from branch 1 is mapped to 4 and the priority of data packets from branch 2 is mapped to 2. By doing this, Switch provides differentiated services.

Figure 5-1 Networking diagram of priority mapping based on simple traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure interfaces so that branch 1 and branch 2 of the enterprise can access the network through the Switch.
2. Create DiffServ domains and map 802.1p priorities to PHBs and colors.
3. Bind the DiffServ domain to inbound interfaces XGE 0/0/1 and XGE 0/0/2 on the Switch.

Data Preparation

To complete the configuration, you need the following data:

- Names of DiffServ domains
- 802.1p priorities of packets from branch 1 and branch 2 of the enterprise
- CoS of branch 1 and branch 2 of the enterprise

Procedure

Step 1 Create VLANs and configure interfaces.

Create VLANs 100, 200, and 300.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 200 300
```

Configure the type of XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 as trunk, add XGE 0/0/1 to VLAN 100, add XGE 0/0/2 to VLAN 200, and add XGE 0/0/3 to VLAN 100, VLAN 200, and VLAN 300.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-XGigabitEthernet0/0/2] quit
[Switch] interface xgigabitethernet0/0/3
[Switch-XGigabitEthernet0/0/3] port link-type trunk
[Switch-XGigabitEthernet0/0/3] port trunk allow-pass vlan 100 200 300
[Switch-XGigabitEthernet0/0/3] quit
```

Create VLANIF 300 and assign interface IP address uo192.168.1.1/24 to VLANIF 300.

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
```

NOTE

Assign IP address 192.168.1.2/24 to the interface connecting the router and the Switch.

Step 2 Create and configure DiffServ domains.

Create DiffServ domains **ds1** and **ds2** and map 802.1p priorities of packets from branch 1 and branch 2 of the enterprise to PHBs and colors.

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 0 phb af4 green
[Switch-dsdomain-ds1] quit
[Switch] diffserv domain ds2
[Switch-dsdomain-ds2] 8021p-inbound 0 phb af2 green
[Switch-dsdomain-ds2] quit
```

Step 3 Bind DiffServ domains to interfaces.

Bind DiffServ domains **ds1** and **ds2** to XGE 0/0/1, and XGE 0/0/2 respectively.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] trust upstream ds1
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] trust upstream ds2
[Switch-XGigabitEthernet0/0/2] quit
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 100 200 300
#
diffserv domain ds1
  8021p-inbound 0 phb af4 green
#
diffserv domain ds2
  8021p-inbound 0 phb af2 green
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 trust upstream ds1
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 trust upstream ds2
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200 300
#
return
```

5.1.2 Example for Re-marking the Priorities Based on Complex Traffic Classification

After priority re-marking based on complex traffic classification is configured, the S6700 adds the same outer VLAN ID to packets with different VLAN IDs. That is, these packets are uniformly taken as the service data. In addition, the S6700 re-marks different 802.1p priorities of packets with different VLAN IDs to provide differentiated services.

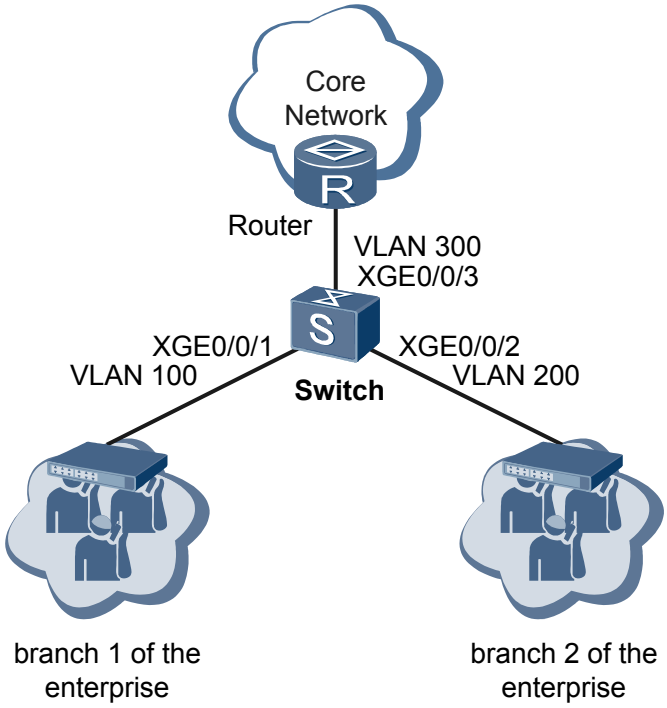
Networking Requirements

The Switch is connected to the router through XGE 0/0/3; branch 1 and branch 2 of the enterprise can access the network through the Switch and router. See **Figure 5-2**.

Data services of branch 1 and branch 2 of the enterprise come from VLANs 100 and 200. When the data service packets of branch 1 and branch 2 of the enterprise pass the Switch, the Switch needs to add the outer VLAN tag with the VLAN 300 to the packets so that these packets are identified as data services on the Core network. In addition, branch 1 require better QoS

guarantee; therefore, the priority of data packets to branch 1 is mapped to 4 and the priority of data packets to branch 2 is mapped to 2. By doing this, differentiated services are provided.

Figure 5-2 Networking diagram of priority re-marking based on complex traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure interfaces so that branch 1 and branch 2 of the enterprise can access the network through the Switch.
2. Create traffic classifiers based on the VLAN ID in the inner VLAN tag on the Switch.
3. Create traffic behaviors on the Switch and re-mark 802.1p priorities of packets.
4. Create a traffic policy on the Switch, bind traffic behaviors to traffic classifiers in the traffic policy, and apply the traffic policy to the interface at the inbound direction.

Data Preparation

To complete the configuration, you need the following data:

- Re-marked priorities of packets with different VLAN IDs in the inner VLAN tags
- Type, direction, and number of the interface that a traffic policy needs to be applied to

Procedure

Step 1 Create VLANs and configure interfaces.

Create VLANs 100, 200, and 300 on the Switch and configure the interfaces so that the Switch adds the outer VLAN tag with the VLAN ID as 300 to the packets sent from XGE 0/0/1 and XGE 0/0/2 and XGE 0/0/3 can forward packets in VLAN 300.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 200 300
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port hybrid pivd vlan 100
[Switch-XGigabitEthernet0/0/1] port hybrid untagged vlan 100 300
[Switch-XGigabitEthernet0/0/1] qinq vlan-translation enable
[Switch-XGigabitEthernet0/0/1] port vlan-stacking vlan 100 stack-vlan 300
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port hybrid pivd vlan 200
[Switch-XGigabitEthernet0/0/1] port hybrid untagged vlan 200 300
[Switch-XGigabitEthernet0/0/2] qinq vlan-translation enable
[Switch-XGigabitEthernet0/0/2] port vlan-stacking vlan 200 stack-vlan 300
[Switch-XGigabitEthernet0/0/2] quit
[Switch] interface xgigabitethernet0/0/3
[Switch-XGigabitEthernet0/0/3] port link-type trunk
[Switch-XGigabitEthernet0/0/3] port trunk allow-pass vlan 300
[Switch-XGigabitEthernet0/0/3] quit
```

Create VLANIF 300 and assign IP address 192.168.1.1/24 to VLANIF 300.

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
[Switch-Vlanif300] quit
```

Step 2 Create traffic classifiers.

Create traffic classifiers **c1** to **c2** on the Switch to classify incoming packets based on the VLAN ID in the inner VLAN tag.

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match cvlan-id 100
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match cvlan-id 200
[Switch-classifier-c2] quit
```

Step 3 Create traffic behaviors.

Create traffic behaviors **b1** to **b2** on the Switch to re-mark priorities of user packets.

```
[Switch] traffic behavior b1
[Switch-behavior-b1] remark 8021p 4
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] remark 8021p 2
[Switch-behavior-b2] quit
```

Step 4 Create a traffic policy and apply it to an interface.

Create traffic policy **p1** on the Switch, bind traffic classifiers to traffic behaviors in the traffic policy, and apply the traffic policy to XGE 0/0/1 andXGE 0/0/2 in the inbound direction to re-mark priorities of packets coming from the user side.

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] quit
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] traffic-policy p1 inbound
[Switch-XGigabitEthernet0/0/2] quit
```

Step 5 Verify the configuration.

Check the configuration of traffic classifiers.

```
<Switch> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: AND
    Rule(s) : if-match cvlan-id 200

   Classifier: c1
    Operator: AND
    Rule(s) : if-match cvlan-id 100
```

Check the configuration of the traffic policy.

```
<Switch> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Marking:
        Remark 8021p 4
   Classifier: c2
    Operator: AND
     Behavior: b2
      Marking:
        Remark 8021p 2
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 100 200 300
#
traffic classifier c2 operator and
 if-match cvlan-id 200
traffic classifier c1 operator and
 if-match cvlan-id 100
#
traffic behavior b2
 remark 8021p 2
traffic behavior b1
 remark 8021p 4
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 qinq vlan-translation enable
 port hybrid pvid vlan
100
 port hybrid untagged vlan 100 300
 port vlan-stacking vlan 100 stack-vlan 300
 traffic-policy p1 inbound
#
interface XGigabitEthernet0/0/2
 qinq vlan-translation enable
 port hybrid pvid vlan
200
 port hybrid untagged vlan 200 300
 port vlan-stacking vlan 200 stack-vlan 300
```

```
 traffic-policy p1 inbound
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
return
```

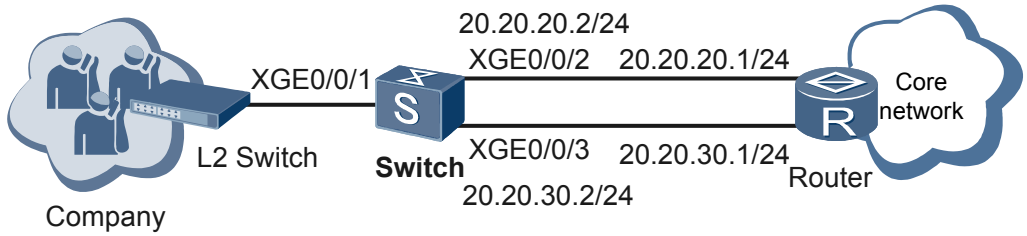
5.1.3 Example for Configuring Policy-based Routing

After packet redirection based on complex traffic classification is configured, the S6700 redirects packets with different IP priorities to different interfaces so that the S6700 provides different bandwidth services.

Networking Requirements

The Layer 2 switch of a company is connected to the ISP device through the Switch; one is a 1-Gbit/s link with the gateway as 20.20.20.1/24 and the other is a 10-Gbit/s link with the gateway as 20.20.30.1/24. The company requires that the 10 Gbit/s links send only the packets with priorities as 4, 5, 6, and 7 and 1 Gbit/s links send packets of lower priorities to the ISP. See **Figure 5-3**.

Figure 5-3 Policy-based routing networking



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure interfaces so that the Switch can ping the ISP device.
2. Create ACL rules to match the packets with priorities as 4, 5, 6, and 7 and priorities as 0, 1, 2, and 3.
3. Create traffic classifiers to match the preceding ACL rules.
4. Create traffic behaviors to redirect matching packets to 20.20.20.1/24 and 20.20.30.1/24.
5. Create a traffic policy, bind traffic classifiers to traffic behaviors in the traffic policy, and apply the traffic policy to an interface.

Data Preparation

To complete the configuration, you need the following data:

- VLAN 20 and VLAN 30 that all of XGE0/0/1, XGE0/0/2 and XGE0/0/3 are added to
- ACL rules 3001 and 3002
- Traffic classifiers **c1** and **c2**

- Traffic behaviors **b1** and **b2**
- Traffic policy **p1**

Procedure

Step 1 Create VLANs and configure interfaces.

Create VLANs 20 and 30.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 20 30
```

Configure the type of XGE 0/0/1, XGE 0/0/2 and XGE 0/0/3 to trunk, and add all of XGE 0/0/1, XGE 0/0/2 and XGE 0/0/3 to VLAN 20 and VLAN 30.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 20 30
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 20 30
[Switch-XGigabitEthernet0/0/2] quit
[Switch] interface xgigabitethernet0/0/3
[Switch-XGigabitEthernet0/0/3] port link-type trunk
[Switch-XGigabitEthernet0/0/3] port trunk allow-pass vlan 20 30
[Switch-XGigabitEthernet0/0/3] quit
```

Create VLANIF 20 and VLANIF 30 and assign IP addresses to them.

```
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 20.20.20.2 24
[Switch-Vlanif20] quit
[Switch] interface vlanif 30
[Switch-Vlanif30] ip address 20.20.30.2 24
[Switch-Vlanif30] quit
```

NOTE

Assign network segment addresses 20.20.20.1/24 and 20.20.30.1/24 to the interfaces connecting the router and Switch. The details are not mentioned here.

Step 2 Create ACL rules.

Create advanced ACL rules 3001 and 3002 on the Switch to permit the packets with priorities as 4, 5, 6, and 7 and priorities as 0, 1, 2, and 3 to pass through.

```
[Switch] acl 3001
[Switch-acl-adv-3001] rule permit ip precedence 0
[Switch-acl-adv-3001] rule permit ip precedence 1
[Switch-acl-adv-3001] rule permit ip precedence 2
[Switch-acl-adv-3001] rule permit ip precedence 3
[Switch-acl-adv-3001] quit
[Switch] acl 3002
[Switch-acl-adv-3002] rule permit ip precedence 4
[Switch-acl-adv-3002] rule permit ip precedence 5
[Switch-acl-adv-3002] rule permit ip precedence 6
[Switch-acl-adv-3002] rule permit ip precedence 7
[Switch-acl-adv-3002] quit
```

Step 3 Create traffic classifiers.

Create traffic classifiers **c1** and **c2** on the Switch with matching rules as ACL 3001 and ACL 3002.

```
[Switch] traffic classifier c1
```

```
[Switch-classifier-c1] if-match acl 3001
[Switch-classifier-c1] quit
[Switch] traffic classifier c2
[Switch-classifier-c2] if-match acl 3002
[Switch-classifier-c2] quit
```

Step 4 Create traffic behaviors.

Create traffic behaviors **b1** and **b2** on the Switch to redirect packets to network segments 20.20.20.1/24 and 20.20.30.1/24.

```
[Switch] traffic behavior b1
[Switch-behavior-b1] redirect ip-nexthop 20.20.20.1
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] redirect ip-nexthop 20.20.30.1
[Switch-behavior-b2] quit
```

Step 5 Create a traffic policy and apply it to an interface.

Create traffic policy **p1** on the Switch and bind traffic classifiers to traffic behaviors in the traffic policy.

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] quit
```

Apply traffic policy **p1** to XGE 0/0/1.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-XGigabitEthernet0/0/1] quit
[Switch] quit
```

Step 6 Verify the configuration.

Check the configuration of ACL rules.

```
[Switch] display acl 3001
Advanced ACL 3001, 4 rules
Acl's step is 5
 rule 5 permit ip precedence routine
 rule 10 permit ip precedence priority
 rule 15 permit ip precedence immediate
 rule 20 permit ip precedence flash
[Switch] display acl 3002
Advanced ACL 3002, 4 rules
Acl's step is 5
 rule 5 permit ip precedence flash-override
 rule 10 permit ip precedence critical
 rule 15 permit ip precedence internet
 rule 20 permit ip precedence network
```

Check the configuration of traffic classifiers.

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: AND
    Rule(s) : if-match acl 3002

   Classifier: c1
    Operator: AND
    Rule(s) : if-match  acl 3001


Total classifier number is 2
```

View the configuration of the traffic policy.

```
<Switch> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Redirect:
        Redirect ip-nexthop
        20.20.20.1
   Classifier: c2
    Operator: AND
     Behavior: b2
      Redirect:
        Redirect ip-nexthop
        20.20.30.1
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 20 30
#
acl number 3001
 rule 5 permit ip precedence routine
 rule 10 permit ip precedence priority
 rule 15 permit ip precedence immediate
 rule 20 permit ip precedence flash
#
acl number 3002
 rule 5 permit ip precedence flash-override
 rule 10 permit ip precedence critical
 rule 15 permit ip precedence internet
 rule 20 permit ip precedence network
#
traffic classifier c1 operator and
 if-match acl 3001
traffic classifier c2 operator and
 if-match acl 3002
#
traffic behavior b1
 redirect ip-nexthop 20.20.20.1
traffic behavior b2
 redirect ip-nexthop 20.20.30.1
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
#
interface Vlanif20
 ip address 20.20.20.2 255.255.255.0
#
interface Vlanif30
 ip address 20.20.30.2 255.255.255.0
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 30
 traffic-policy p1 inbound
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 30
#
interface XGigabitEthernet0/0/3
```

```
 port link-type trunk
 port trunk allow-pass vlan 20 30
#
return
```

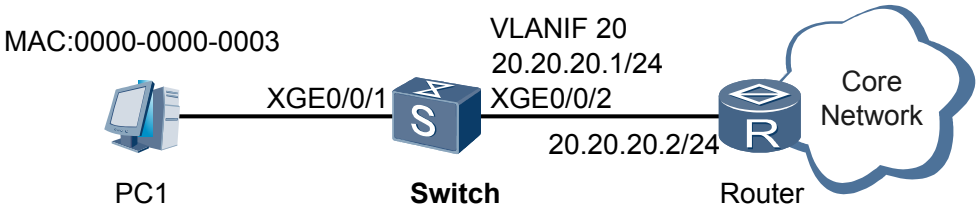
5.1.4 Example for Configuring Traffic Statistics Based on Complex Traffic Classification

After traffic statistics based on complex traffic classification is configured, the S6700 collect traffic statistics on packets with the specified source MAC address.

Networking Requirements

PC1 with the MAC address as 0000-0000-0003 is connected to other devices through XGE0/0/1 on the Switch. It is required that the Switch should take the statistics on the packets with the source MAC address as 0000-0000-0003. See **Figure 5-4**.

Figure 5-4 Networking diagram for configuring traffic statistics based on complex traffic classification



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure interfaces so that the Switch is connected to PC1 and the router.
2. Create an ACL to match the packets with the source MAC address as 0000-0000-0003.
3. Create a traffic classifier to match the ACL.
4. Create a traffic behavior to take the statistics on the matching packets.
5. Create a traffic policy, bind the traffic classifier to the traffic behavior in the traffic policy, and apply the traffic policy to XGE0/0/1 in the inbound direction.

Data Preparation

To complete the configuration, you need the following data:

- VLAN 20
- ACL 4000
- Traffic classifier **c1**
- Traffic behavior **b1**
- Traffic policy **p1**

Procedure

Step 1 Create a VLAN and configure interfaces.

Create VLAN 20.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 20
[Switch-vlan20] quit
```

Configure the type of XGE0/0/1 as access and XGE0/0/2 as trunk, and add XGE0/0/1 and XGE0/0/2 to VLAN 20.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type access
[Switch-XGigabitEthernet0/0/1] port default vlan 20
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 20
[Switch-XGigabitEthernet0/0/2] quit
```

Create VLANIF 20 and assign IP address 20.20.20.1/24 to it.

```
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 20.20.20.1 24
[Switch-Vlanif20] quit
```

NOTE

Assign network segment address 20.20.20.2/24 to the interface connecting the router and Switch. The details are not mentioned here.

Step 2 Create an ACL.

Create Layer 2 ACL 4000 on the Switch to match the packets with the source MAC address as 0000-0000-0003.

```
[Switch] acl 4000
[Switch-acl-L2-4000] rule permit source-mac 0000-0000-0003 ffff-ffff-ffff
[Switch-acl-L2-4000] quit
```

Step 3 Create a traffic classifier.

Create traffic classifier **c1** on the Switch with ACL 4000 as the matching rule.

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 4000
[Switch-classifier-c1] quit
```

Step 4 Create a traffic behavior.

Create traffic behavior **b1** on the Switch and configure the traffic statistics action.

```
[Switch] traffic behavior b1
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
```

Step 5 Create a traffic policy and apply it to an interface.

Create traffic policy **p1** on the Switch and bind the traffic classifier to the traffic behavior in the traffic policy.

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

Apply traffic policy **p1** to XGE0/0/1.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-XGigabitEthernet0/0/1] quit
[Switch] quit
```

Step 6 Verify the configuration.

Check the configuration of the ACL.

```
<Switch> display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 permit source-mac 0000-0000-0003
```

Check the configuration of the traffic classifier.

```
<Switch> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: AND
    Rule(s) : if-match  acl 4000
Total classifier number is 1
```

View the configuration of the traffic policy.

```
<Switch> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      statistic: enable
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 20
#
acl number 4000
 rule 5 permit source-mac 0000-0000-0003
#
traffic classifier c1 operator and
 if-match acl 4000
#
traffic behavior b1
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
#
interface Vlanif20
 ip address 20.20.20.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 20
 traffic-policy p1 inbound
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

5.2 Traffic Policing and Traffic Shaping Configuration

This document describes basic concepts of traffic policing and traffic shaping, and introduces the configuration method of traffic policing based on a traffic classifier, and traffic shaping, and provides configuration examples.

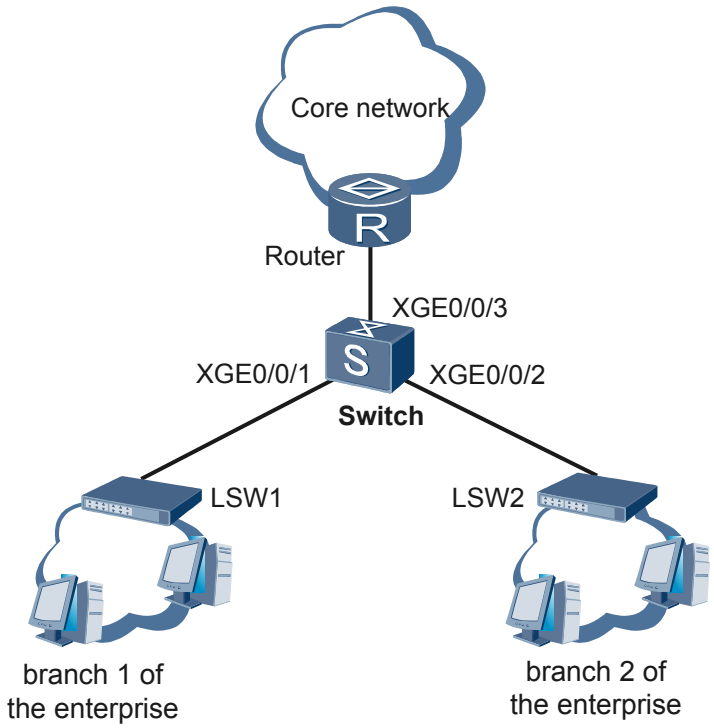
5.2.1 Example for Configuring Traffic Policing Based on an Interface

You can configure interface-based traffic policing so that the Switch can provide different bandwidth services for users.

Networking Requirements

As shown in **Figure 5-5**, the Switch is connected to XGE 0/0/3 through the router; branch 1 and branch 2 of the enterprise are connected to the Switch through XGE 0/0/1 and XGE 0/0/2 and access the network through the Switch and router. Branch 1 and branch 2 of the enterprise require 8 Mbit/s and 5 Mbit/s bandwidth.

Figure 5-5 Networking diagram of traffic policing



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure interfaces of the Switch so that users can access the network.
2. Configure traffic policing on XGE 0/0/1 and XGE 0/0/2 of the Switch in the inbound direction.

Data Preparation

To complete the configuration, you need the following data:

- Uplink interface address of the Switch: 192.168.1.1/24
- VLAN IDs of branch 1 and branch 2 of the enterprise: VLAN 100 and VLAN 200
- CIR of branch 1: 8192 kbit/s; CIR of branch 2: 5120 kbit/s

Procedure

Step 1 Create VLANs and configure interfaces of the Switch.

Create VLANs 100, 200, and 300, and then add XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 to VLANs 100, 200, and 300.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 200 300
```

Set the type of XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 to trunk and configure XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 to allow packets from VLANs 100, 200, and 300 to pass through.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-XGigabitEthernet0/0/2] quit
[Switch] interface xgigabitethernet0/0/3
[Switch-XGigabitEthernet0/0/3] port link-type trunk
[Switch-XGigabitEthernet0/0/3] port trunk allow-pass vlan 100 200 300
[Switch-XGigabitEthernet0/0/3] quit
```

Create VLANIF 300 and set its network segment address to 192.168.1.1/24.

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
[Switch-Vlanif300] quit
```

NOTE

On the router, set the IP address of the interface connecting the router and Switch to 192.168.1.2/24.

Step 2 Configure interface-based traffic policing.

Configure traffic policing on XGE 0/0/1 and XGE 0/0/2 of the Switch.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] qos lr inbound cir 8192
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] qos lr inbound cir 5120
[Switch-XGigabitEthernet0/0/2] quit
[Switch] quit
```

Step 3 Verify the configuration.

View the traffic policing configuration.

```
[Switch] display qos lr inbound interface xgigabitethernet0/0/1
 XGigabitEthernet0/0/1 lr inbound:
  cir: 8192 Kbps, cbs: 1024000 Byte
[Switch] display qos lr inbound interface xgigabitethernet0/0/2
 XGigabitEthernet0/0/2 lr inbound:
  cir: 5120 Kbps, cbs: 640000 Byte
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 100 200 300
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 qos lr inbound cir 8192 cbs 1024000
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 qos lr inbound cir 5120 cbs 640000
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200 300
#

return
```

5.2.2 Example for Configuring Traffic Policing Based on a Traffic Classifier

The Switch provides different bandwidth by configuring traffic policing based on a traffic classifier and setting different CAR parameters.

Networking Requirements

The Switch is connected to the router by using XGE 0/0/2; enterprise users can access the network by using the Switch and the router. See **Table 5-1**.

- Voice services of the enterprise belong to VLAN 120.
- Video services of the enterprise belong to VLAN 110.
- Data services of the enterprise belong to VLAN 100.

On the Switch, traffic policing needs to be performed on packets of different services to limit traffic within a proper range and ensure bandwidth of each service.

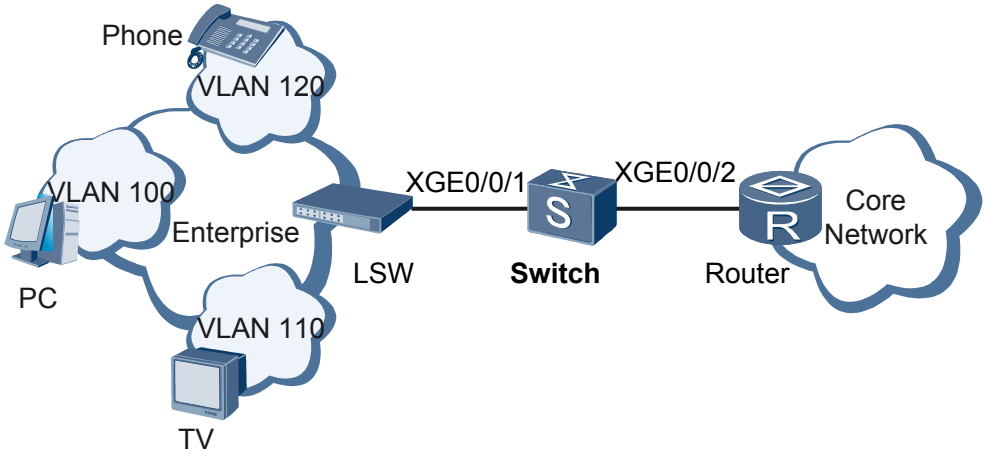
DSCP priorities carried in service packets sent from the user side cannot be trusted and services require different QoS in practice. Therefore, you need to re-mark DSCP priorities of different service packets on the Switch so that the downstream router can process packets based on priorities.

The requirements are as follows:

Table 5-1 QoS provided by the Switch for upstream traffic

Traffic Type	CIR (Mbit/s)	PIR (Mbit/s)	DSCP Priority
Voice	2	10	46
Video	4	10	30
Data	4	10	14

Figure 5-6 Network diagram for configuring traffic policing based on a traffic classifier



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure interfaces so that enterprise can access the network by using the Switch.
2. Create traffic classifiers based on the VLAN ID on the Switch.
3. Create traffic behaviors on the Switch to limit the traffic received from the enterprise and re-mark DSCP priorities of packets.
4. Create a traffic policy on the Switch, bind traffic behaviors to traffic classifiers in the traffic policy, and apply the traffic policy to the interface between the enterprise and the Switch.

Data Preparation

To complete the configuration, you need the following data:

- Names of traffic classifiers matching service flows
- Re-marked priorities of packets with different VLAN IDs
- Parameters for packets with different VLAN IDs: CIR and PIR values
- Type and number of the interface to which a traffic policy needs to be applied

Procedure

Step 1 Create VLANs and configure interfaces.

Create VLAN 100, VLAN 110, and VLAN 120 on the Switch.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 100 110 120
```

Configure the access types of XGE 0/0/1 and XGE0/0/2 to trunk, add XGE 0/0/1 and XGE0/0/2 to VLAN 100, VLAN 110, and VLAN 120.

```
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 110 120
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet 0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 110 120
[Switch-XGigabitEthernet0/0/2] quit
```

Step 2 Create traffic classifiers.

Create traffic classifiers **c1** to **c3** on the Switch to match different service flows from the enterprise based on VLAN IDs.

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match vlan-id 120
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match vlan-id 110
[Switch-classifier-c2] quit
[Switch] traffic classifier c3 operator and
[Switch-classifier-c3] if-match vlan-id 100
[Switch-classifier-c3] quit
```

Step 3 Create traffic behaviors.

Create traffic behaviors **b1** to **b3** on the Switch to limit different service flows and re-mark priorities.

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 2000 pir 10000 green pass
[Switch-behavior-b1] remark dscp 46
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] car cir 4000 pir 10000 green pass
[Switch-behavior-b2] remark dscp 30
[Switch-behavior-b2] statistic enable
[Switch-behavior-b2] quit
[Switch] traffic behavior b3
[Switch-behavior-b3] car cir 4000 pir 10000 green pass
[Switch-behavior-b3] remark dscp 14
[Switch-behavior-b3] statistic enable
[Switch-behavior-b3] quit
```

Step 4 Create a traffic policy and apply it on the interface.

Create traffic policy **p1** on the Switch, bind traffic classifiers to traffic behaviors in the traffic policy, and apply the traffic policy to XGE0/0/1 in the inbound direction to limit the packets received from the user side and re-mark priorities of these packets.

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
```

```
[Switch-trafficpolicy-p1] classifier c3 behavior b3
[Switch-trafficpolicy-p1] quit
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-XGigabitEthernet0/0/1] quit
```

Step 5 Verify the configuration.

Check the configuration of the traffic classifier.

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: AND
    Rule(s) : if-match vlan-id 110

   Classifier: c3
    Operator: AND
    Rule(s) : if-match vlan-id 100

   Classifier: c1
    Operator: AND
    Rule(s) : if-match vlan-id 120

Total classifier number is 3
```

Check the configuration of the traffic policy. Here, the configuration of the traffic policy **p1** is displayed.

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
        Committed Access Rate:
        CIR 2000 (Kbps), CBS 250000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Marking:
        Remark DSCP ef
      statistic: enable
   Classifier: c2
    Operator: AND
     Behavior: b2
        Committed Access Rate:
        CIR 4000 (Kbps), CBS 500000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Marking:
        Remark DSCP af33
      statistic: enable
   Classifier: c3
    Operator: AND
     Behavior: b3
        Committed Access Rate:
        CIR 4000 (Kbps), CBS 500000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Marking:
        Remark DSCP af13
      statistic: enable
```

Check the configuration of the traffic policy applied on an interface. Here, the configuration of the traffic policy applied to XGE0/0/1 is displayed.

```
[Switch] display traffic policy statistics interface xgigabitethernet 0/0/1
inbound

 Interface: XGigabitEthernet0/0/1
 Traffic policy inbound: p1
 Rule number: 3
 Current status: OK!
-----------------------------------------------------------------------
 Board : 0
Item                                Packets                       Bytes
-----------------------------------------------------------------------
Matched                                  10                       10000
  +--Passed                              8                        8000
  +--Dropped                             2                        2000
    +--Filter                            2                        2000
    +--URPF                              0                        0
    +--CAR                               2                        2000
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 100 110 120
#
traffic classifier c1 operator and
 if-match vlan-id 120
traffic classifier c2 operator and
 if-match vlan-id 110
traffic classifier c3 operator and
 if-match vlan-id 100
#
traffic behavior b1
 car cir 2000 pir 10000 cbs 250000 pbs 1250000 green pass yellow pass red
discard
 remark dscp ef
 statistic enable
traffic behavior b2
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 green pass yellow pass red
discard
 remark dscp af33
 statistic enable
traffic behavior b3
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 green pass yellow pass red
discard
 remark dscp af13
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 traffic-policy p1 inbound
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
```

```
#
return
```

5.2.3 Example for Configuring Traffic Shaping

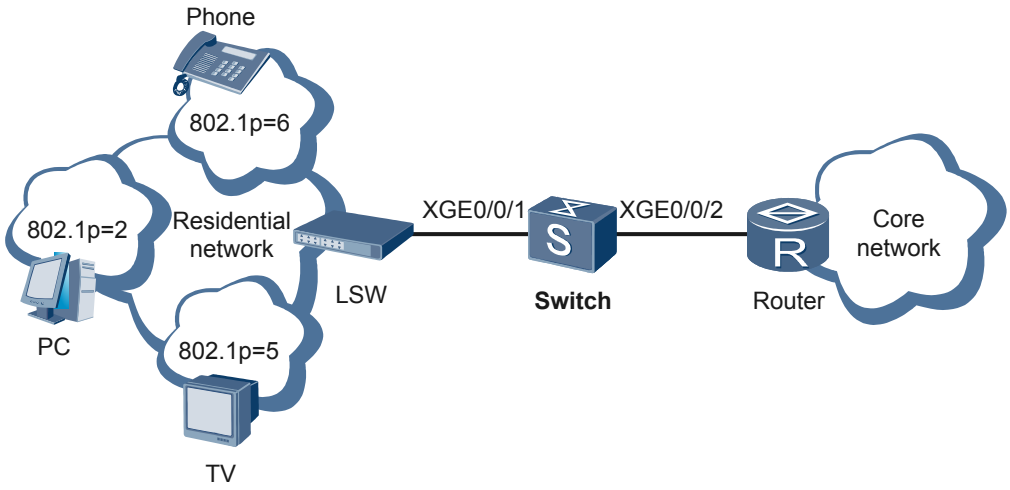
You can configure traffic shaping and set different traffic shaping rates for different types of packets to reduce the jitter and ensure bandwidth of various services.

Networking Requirements

The Switch is connected to XGE 0/0/2 and the router; the 802.1p priorities of voice, video, and data services from the Internet are 6, 5, and 2 respectively, and these services can reach users through the router and Switch, as shown in **Figure 5-7**. The rate of the traffic from the network side is greater than the rate of the LSW interface; therefore, a jitter may occur in the outbound direction of XGE 0/0/1. To reduce the jitter and ensure the bandwidth of various services, the requirements are as follows:

- The CIR on the interface is 20000 kbit/s.
- The CIR and PIR for the voice service are 3000 kbit/s and 5000 kbit/s respectively.
- The CIR and PIR for the video service are 5000 kbit/s and 8000 kbit/s respectively.
- The CIR and PIR for the data service are 2000 kbit/s and 3000 kbit/s respectively.

Figure 5-7 Networking diagram for configuring traffic shaping



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and configure each interface so that the residential user can access the network through the Switch.
2. Configure interfaces to trust 802.1p priorities of packets.
3. Configure traffic shaping on an interface to limit the bandwidth of the interface.
4. Configure traffic shaping in an interface queue to limit the CIRs of voice, video, and data services.

Data Preparation

To complete the configuration, you need the following data:

- 802.1p priorities
- Rate for traffic shaping on an interface
- Rate for traffic shaping in each interface queue

Procedure

Step 1 Create VLANs and configure interfaces.

Create VLAN 10.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 10
```

Set the type of XGE 0/0/1 and XGE 0/0/2 to trunk, and then add XGE 0/0/1 and XGE 0/0/2 to VLAN 10.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Switch-XGigabitEthernet0/0/2] quit
```

Create VLANIF 10 and assign network segment address 10.10.10.1/24 to VLANIF 10.

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.10.10.1 255.255.255.0
[Switch-Vlanif10] quit
```

NOTE

Assign IP address 10.10.10.2/24 to the interface connecting the router and Switch.

Step 2 Configure traffic shaping on an interface.

Configure traffic shaping on an interface of the Switch and set the CIR to 20000 kbit/s.

```
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] qos lr outbound cir 20000 cbs 2500000
```

Step 3 Configure traffic shaping in an interface queue.

Set the scheduling mode of each queue to WRR. Set the WRR weight of queue 6 to 60, WRR weight of queue 5 to 40, and WRR weight of queue 2 to 20. The other queues retain the default weight.

```
[Switch-XGigabitEthernet0/0/1] qos wrr
[Switch-XGigabitEthernet0/0/1] qos queue 6 wrr weight 60
[Switch-XGigabitEthernet0/0/1] qos queue 5 wrr weight 40
[Switch-XGigabitEthernet0/0/1] qos queue 2 wrr weight 20
```

Configure traffic shaping in the interface queues on the Switch, and then set the CIR and PIR of the voice service to 3000 kbit/s and 5000kbit/s, the CIR and PIR of the video service to 5000 kbit/s and 8000 kbit/s, and the CIR and PIR of the data service to 2000 kbit/s and 3000 kbit/s.

```
[Switch-XGigabitEthernet0/0/1] qos queue 6 shaping cir 3000 pir 5000
[Switch-XGigabitEthernet0/0/1] qos queue 5 shaping cir 5000 pir 8000
[Switch-XGigabitEthernet0/0/1] qos queue 2 shaping cir 2000 pir 3000
```

```
[Switch-XGigabitEthernet0/0/1] quit
[Switch] quit
```

Step 4 Verify the configuration.

If the configuration succeeds, the committed bandwidth for the packets transmitted by GE0/0/1 is 20000 kbit/s; the transmission rate of the voice service ranges from 3000 kbit/s to 5000 kbit/s; the transmission rate of the video service ranges from 5000 kbit/s to 8000 kbit/s; the transmission rate of the data service ranges from 2000 kbit/s to 3000 kbit/s.

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 qos lr outbound cir 20000 cbs 2500000
 qos wrr
 qos queue 2 wrr weight 20
 qos queue 5 wrr weight 40
 qos queue 6 wrr weight 60
 qos queue 2 shaping cir 2000 pir 3000
 qos queue 5 shaping cir 5000 pir 8000
 qos queue 6 shaping cir 3000 pir 5000
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

5.3 Congestion Avoidance and Congestion Management Configuration

This chapter describes the basic concepts of congestion avoidance and congestion management, and provides configuration methods and configuration examples of congestion avoidance and congestion management.

5.3.1 Example for Configuring Congestion Avoidance and Congestion Management

After congestion avoidance and congestion management are configured, the S6700 provides different services for packets of different priorities and ensures high-priority and low-delay services.

Networking Requirements

The Switch is connected to the router through XGE 0/0/3; the 802.1p priorities of voice, video, and data services on the Internet are 6, 5, and 2 respectively, and these services can reach users

through the router and Switch, as shown in **Figure 5-8**. The rate of incoming interface XGE 0/0/3 on the Switch is greater than the rates of outgoing interfaces XGE 0/0/1 and XGE 0/0/2; therefore, congestion may occur on these two outgoing interfaces. To reduce the effect caused by congestion and ensure that high-priority and short-delay services are processed first, the requirements are as follows.

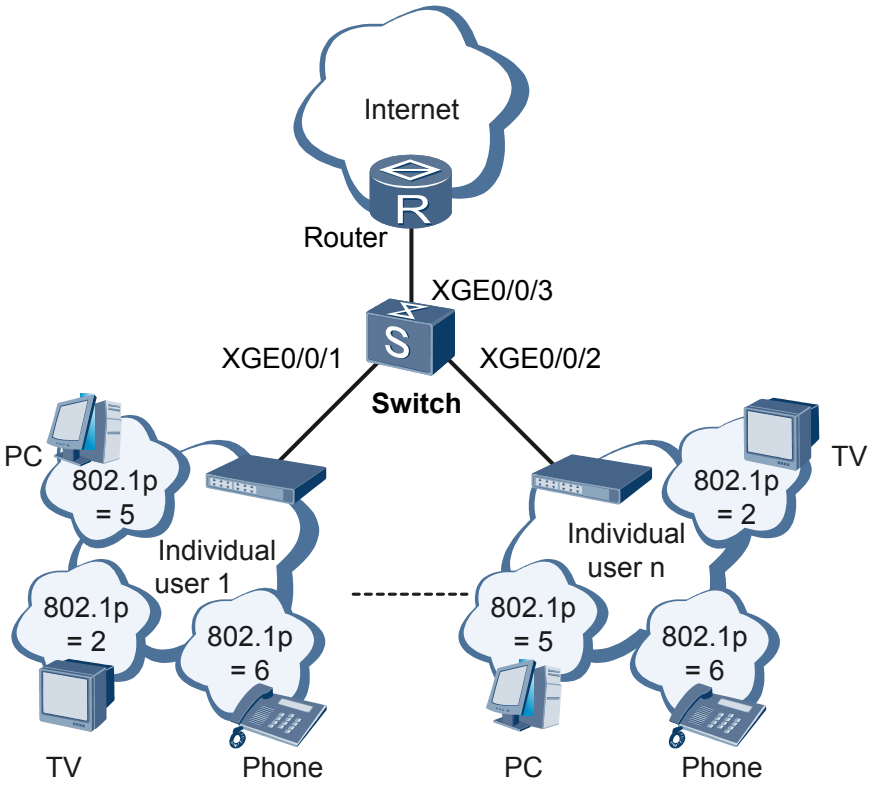
Table 5-2 Congestion avoidance parameters

Types of Services	Color	Lower Threshold (%)	Upper Threshold (%)	Drop Percent
Voice	Green	80	100	10
Video	Yellow	60	80	20
Data	Red	40	60	40

Table 5-3 Congestion management parameters

Type of Services	CoS
Voice	EF
Video	AF3
Data	AF1

Figure 5-8 Networking diagram for configuring congestion avoidance and congestion management



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the VLAN for each interface so that the devices can communicate with each other.
2. Create and configure a DiffServ domain on the Switch, map packets of 802.1p priorities to PHBs and colors of packets, and bind the DiffServ domain to an incoming interface on the Switch.
3. Create a WRED drop profile on the Switch and apply the WRED drop profile on an outgoing interface.
4. Set scheduling parameters of queues of different CoS on outgoing interfaces of the Switch.

Data Preparation

To complete the configuration, you need the following data:

- VLAN IDs of data packets, video packets, and voice packets, namely, 2, 5, and 6
- PHBs mapped to 802.1p priorities being 6, 5, and 2 and colors
- Name of the WRED drop profile and WRED parameters
- Scheduling parameters of queues of different CoS

Procedure

Step 1 Configure the VLAN for each interface so that the devices can communicate with each other.

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan batch 2 5 6
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2 5 6
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] port link-type trunk
[Switch-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 5 6
[Switch-XGigabitEthernet0/0/2] quit
[Switch] interface xgigabitethernet0/0/3
[Switch-XGigabitEthernet0/0/3] port link-type trunk
[Switch-XGigabitEthernet0/0/3] port trunk allow-pass vlan 2 5 6
[Switch-XGigabitEthernet0/0/3] quit
```

Step 2 Configure priority mapping based on simple traffic classification.

Create DiffServ domain **ds1**, map packets of 802.1p priorities being 6, 5, and 2 to PHBs CS6, EF, and AF2, and color packets as green, yellow, and red.

```
[Quidway] sysname Switch
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 6 phb ef green
[Switch-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[Switch-dsdomain-ds1] 8021p-inbound 2 phb af1 red
[Switch-dsdomain-ds1] quit
```

Bind incoming interface XGE 0/0/3 on the Switch to DiffServ domain **ds1**.

```
[Switch] interface xgigabitethernet0/0/3
[Switch-XGigabitEthernet0/0/3] trust upstream ds1
```

```
[Switch-XGigabitEthernet0/0/3] trust 8021p inner
[Switch-XGigabitEthernet0/0/3] quit
```

Step 3 Configure congestion avoidance.

Create drop profile **wred1** on the Switch and set parameters of packets of three colors.

```
[Switch] drop-profile wred1
[Switch-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[Switch-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[Switch-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[Switch-drop-wred1] quit
```

Apply drop profile **wred1** on outgoing interfaces XGE 0/0/1 and XGE 0/0/2 of the Switch.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] qos wred wred1
[Switch-XGigabitEthernet0/0/1] qos queue 5 wred wred1
[Switch-XGigabitEthernet0/0/1] qos queue 3 wred wred1
[Switch-XGigabitEthernet0/0/1] qos queue 1 wred wred1
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] qos wred wred1
[Switch-XGigabitEthernet0/0/2] qos queue 5 wred wred1
[Switch-XGigabitEthernet0/0/2] qos queue 3 wred wred1
[Switch-XGigabitEthernet0/0/2] qos queue 1 wred wred1
[Switch-XGigabitEthernet0/0/2] quit
```

Step 4 Configure congestion management.

Set scheduling parameters of queues of different CoS on outgoing interfaces XGE 0/0/1 and XGE 0/0/2 of the Switch.

```
[Switch] interface xgigabitethernet0/0/1
[Switch-XGigabitEthernet0/0/1] qos drr
[Switch-XGigabitEthernet0/0/1] qos queue 5 drr weight 0
[Switch-XGigabitEthernet0/0/1] qos queue 3 drr weight 100
[Switch-XGigabitEthernet0/0/1] qos queue 1 drr weight 50
[Switch-XGigabitEthernet0/0/1] quit
[Switch] interface xgigabitethernet0/0/2
[Switch-XGigabitEthernet0/0/2] qos drr
[Switch-XGigabitEthernet0/0/2] qos queue 5 drr weight 0
[Switch-XGigabitEthernet0/0/2] qos queue 3 drr weight 100
[Switch-XGigabitEthernet0/0/2] qos queue 1 drr weight 50
[Switch-XGigabitEthernet0/0/2] quit
[Switch] quit
```

Step 5 Verify the configuration.

Check the configuration of DiffServ domain **ds1**.

```
<Switch> display diffserv domain name ds1
Diffserv domain name:ds1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 red
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af3 yellow
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb ef green
 8021p-inbound 6 phb cs7 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 ......
```

Check the configuration of drop profile **wred1**.

```
<Switch> display drop-profile name wred1
Drop-profile[3]: wred1
Color     Low-limit   High-limit  Discard-percentage
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
Non-tcp   100         100         100
------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of the Switch

```
#
 sysname Switch
#
 vlan batch 2 5 6
#
diffserv domain ds1
 8021p-inbound 2 phb af1 red
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
#
 drop-profile wred1
  color green low-limit 80 high-limit 100 discard-percentage 10
  color yellow low-limit 60 high-limit 80 discard-percentage 20
  color red low-limit 40 high-limit 60 discard-percentage 40
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 5 6
 qos drr
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
 qos queue 5 drr weight 0
 qos wred wred1
 qos queue 1 wred wred1
 qos queue 3 wred wred1
 qos queue 5 wred wred1
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 5 6
 qos drr
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
 qos queue 5 drr weight 0
 qos wred wred1
 qos queue 1 wred wred1
 qos queue 3 wred wred1
 qos queue 5 wred wred1
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 5 6
 trust upstream ds1
 trust 8021p inner

#
return
```

6 Configuration Guide - Security

About This Chapter

This document describes security features of the S6700 including AAA and user management, Network Access Control (NAC), DHCP snooping, ARP security, IP source guard, IP source trail, Unicast Reverse Path Forwarding (URPF), local attack defense, PPPoE+, MAC-forced forwarding (MFF), traffic suppression, and ACL from aspects of function introduction, configuration methods, maintenance, and configuration examples.

This document guides you through the principle and configuration of security features.

6.1 AAA and User Management Configuration
This chapter describes the principle and configuration of Authentication, Authorization, and Accounting (AAA), local user management, Remote Authentication Dial in User Service (RADIUS), HUAWEI Terminal Access Controller Access Control System (HWTACACS), and domain.

6.2 NAC Configuration
This chapter describes the working principle and configuration of network access control (NAC).

6.3 DHCP Snooping Configuration
This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on the S6700 to defend against DHCP attacks.

6.4 ARP Security Configuration
The ARP security technology ensures security and robustness of network devices by filtering out untrusted ARP packets and perform timestamp suppression for some ARP packets.

6.5 Source IP Attack Defense Configuration
This chapter describes the principle and configuration of attacking IP source addresses.

6.6 Local Attack Defense Configuration
This chapter describes the principle and configuration of local attack defense.

6.7 PPPoE+ Configuration
This chapter describes how to configure PPPoE+.

6.8 MFF Configuration
This section describes the principle and configuration of the MAC-Forced Forwarding (MFF) function.

6.9 Traffic Suppression Configuration

This chapter describes the principle and configuration of traffic suppression .

6.10 ACL Configuration

The ACL classifies packets according to the rules. After these rules are applied to the interfaces on the S6700, the S6700 can determine packets that are received and rejected.

6.11 ND Snooping Configuration

This chapter describes the principle and configuration method of neighbor discovery (ND) snooping and provides configuration examples.

6.1 AAA and User Management Configuration

This chapter describes the principle and configuration of Authentication, Authorization, and Accounting (AAA), local user management, Remote Authentication Dial in User Service (RADIUS), HUAWEI Terminal Access Controller Access Control System (HWTACACS), and domain.

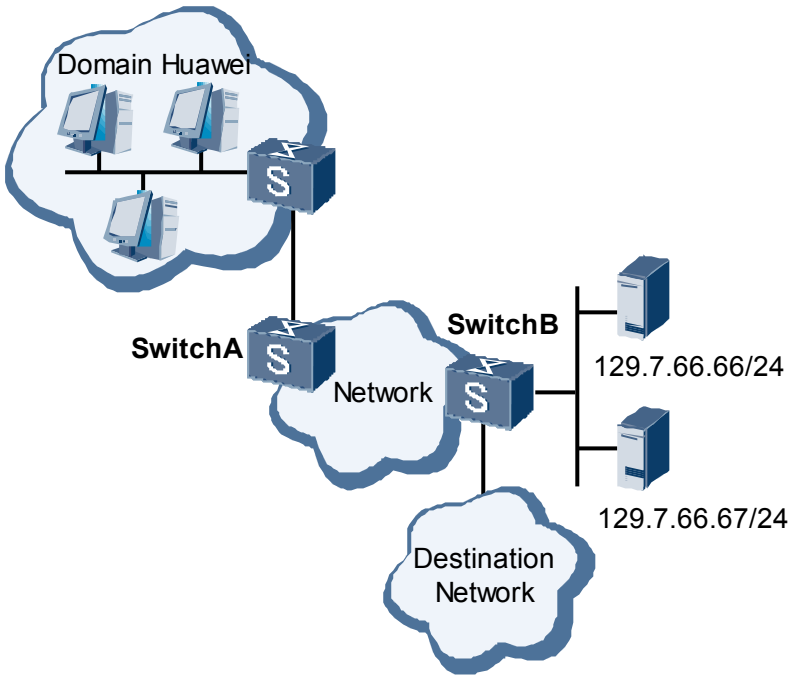
6.1.1 Example for Configuring RADIUS Authentication and Accounting

Networking Requirements

As shown in **Figure 6-1**, users access the network through Switch A and are located in the domain **huawei**. Switch B acts as the network access server of the destination network. The access request of the user needs to pass the network of Switch A and Switch B to reach the authentication server. The user can access the destination network through Switch B after passing the remote authentication. The remote authentication mode on Switch B is as follows:

- The RADIUS server performs authentication and accounting for access users.
- The RADIUS server 129.7.66.66/24 functions as the primary authentication and accounting server. The RADIUS server 129.7.66.67/24 functions as the secondary authentication and accounting server. The default authentication port and accounting port are 1812 and 1813 respectively.

Figure 6-1 Networking diagram of RADIUS authentication and accounting



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a RADIUS server template.
2. Configure the authentication and accounting schemes.
3. Apply the RADIUS server template, the authentication and accounting schemes to the domain.

Data Preparation

To complete the configuration, you need the following data:

- Name of the domain that a user belongs to
- Name of the RADIUS server template
- Name of the authentication scheme, authentication mode, name of the accounting scheme, and accounting mode
- IP addresses, authentication and accounting port numbers of the primary and secondary RADIUS servers
- Key and retransmission times of the RADIUS server

NOTE

The following configurations are performed on Switch B.

Procedure

Step 1 Configure a RADIUS server template.

Configure the RADIUS template named **shiva**.

```
<Quidway> system-view
[Quidway] radius-server template shiva
```

Configure the IP addresses and port numbers of the primary RADIUS authentication and accounting servers.

```
[Quidway-radius-shiva] radius-server authentication 129.7.66.66 1812
[Quidway-radius-shiva] radius-server accounting 129.7.66.66 1813
```

Set the IP addresses and port numbers of the secondary RADIUS authentication and accounting servers.

```
[Quidway-radius-shiva] radius-server authentication 129.7.66.67 1812 secondary
[Quidway-radius-shiva] radius-server accounting 129.7.66.67 1813 secondary
```

Set the key and retransmission count for the RADIUS server.

```
[Quidway-radius-shiva] radius-server shared-key cipher hello
[Quidway-radius-shiva] radius-server retransmit 2
[Quidway-radius-shiva] quit
```

Step 2 Configure the authentication and accounting schemes.

Configure authentication **scheme1**, with the authentication mode being RADIUS.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme 1
Info: Create a new authentication scheme
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

Configure the accounting **scheme1**, with the accounting mode being RADIUS.

```
[Quidway-aaa] accounting-scheme 1
Info: Create a new accounting scheme
[Quidway-aaa-accounting-1] accounting-mode radius
[Quidway-aaa-accounting-1] quit
```

Step 3 Configure the domain **huawei** and apply authentication **scheme1**, accounting **scheme1**, and RADIUS template **shiva** to the domain.

```
[Quidway-aaa] domain huawei
[Quidway-aaa-domain-huawei] authentication-scheme 1
[Quidway-aaa-domain-huawei] accounting-scheme 1
[Quidway-aaa-domain-huawei] radius-server shiva
```

Step 4 Verify the configuration.

After running the **display radius-server configuration template** command on Switch B, you can view that the configuration of the RADIUS server template meets the requirements.

```
<Quidway> display radius-server configuration template shiva
  ------------------------------------------------------------------------
  Server-template-name             :  shiva
  Protocol-version                 :  standard
  Traffic-unit                     :  B
  Shared-secret-key                :  3MQ*TZ,O3KCQ=^Q`MAF4<1!!
  Timeout-interval(in second)      :  5
  Primary-authentication-server    :  129.7.66.66    :1812   LoopBack:NULL
  Primary-accounting-server        :  129.7.66.66    :1813   LoopBack:NULL
  Secondary-authentication-server  :  129.7.66.67    :1812   LoopBack:NULL
  Secondary-accounting-server      :  129.7.66.67    :1813   LoopBack:NULL
  Retransmission                   :  2
  Domain-included                  :  YES
  Calling-station-id MAC-format    :  XX.XX.XX.XX.XX.XX
------------------------------------------------------------------------
```

----End

Configuration Files

```
#
sysname Quidway
#
radius-server template shiva
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 129.7.66.66 1812
 radius-server authentication 129.7.66.67 1812 secondary
 radius-server accounting 129.7.66.66 1813
 radius-server accounting 129.7.66.67 1813 secondary
 radius-server retransmit 2
#
aaa
 authentication-scheme default
 authentication-scheme 1
  authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 accounting-scheme 1
  accounting-mode radius
 domain default
 domain default_admin
 domain huawei
  authentication-scheme 1
  accounting-scheme 1
  radius-server shiva
#
return
```

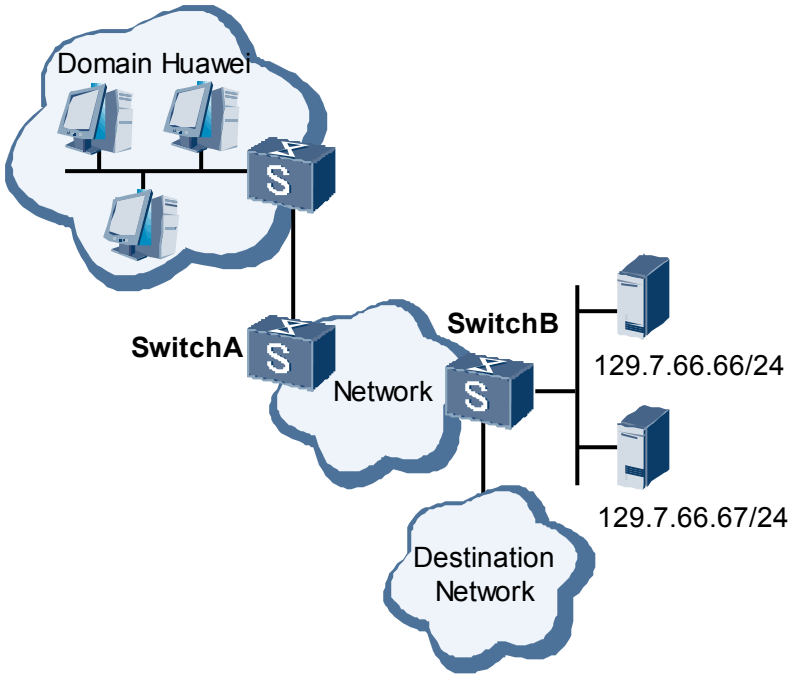
6.1.2 Example for Configuring HWTACACS Authentication, Accounting, and Authorization

Networking Requirements

As shown in **Figure 6-2**:

- The HWTACACS server is adopted to authenticate access users. If HWTACACS server authentication fails, Access users are authenticated locally.
- HWTACACS authentication is required before the level of access users is promoted. If the HWTACACS authentication is not responded, local authentication is performed.
- HWTACACS authorization is performed to access users.
- All access users need to be charged.
- Interim accounting is performed every 3 minutes.
- The primary HWTACACS server is 129.7.66.66/24, and the IP address of the secondary HWTACACS server is 129.7.66.67/24. The port number of the server for authentication, accounting, and authorization is 49.

Figure 6-2 Networking diagram of HWTACACS authentication, accounting, and authorization



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an HWTACACS server template.
2. Configure the authentication, authorization, and accounting schemes.

3. Apply the HWTACACS server template, authentication, authorization, and accounting schemes to the domain.

Data Preparation

To complete the configuration, you need the following data:

- Name of the domain that the user belongs to
- Name of the HWTACACS server template
- Name of the authentication scheme, authentication mode, name of the authorization scheme, authorization mode, name of the accounting scheme, and accounting mode
- IP addresses, authentication port numbers, authorization port numbers, and accounting port numbers of the primary and secondary HWTACACS servers
- Key of the HWTACACS server

NOTE

The following configurations are performed on Switch B.

Procedure

Step 1 Configure an HWTACACS server template.

Configure an HWTACACS server template named **ht**.

```
<Quidway> system-view
[Quidway] hwtacacs-server template ht
```

Configure the IP address and port number of the primary HWTACACS server for authentication, authorization, and accounting.

```
[Quidway-hwtacacs-ht] hwtacacs-server authentication 129.7.66.66 49
[Quidway-hwtacacs-ht] hwtacacs-server authorization 129.7.66.66 49
[Quidway-hwtacacs-ht] hwtacacs-server accounting 129.7.66.66 49
```

Configure the IP address and port number of the secondary HWTACACS server for authentication, authorization, and accounting.

```
[Quidway-hwtacacs-ht] hwtacacs-server authentication 129.7.66.67 49 secondary
[Quidway-hwtacacs-ht] hwtacacs-server authorization 129.7.66.67 49 secondary
[Quidway-hwtacacs-ht] hwtacacs-server accounting 129.7.66.67 49 secondary
```

Configure the key of the TACACS server.

```
[Quidway-hwtacacs-ht] hwtacacs-server shared-key cipher hello
[Quidway-hwtacacs-ht] quit
```

Step 2 Configure the authentication, authorization, and accounting schemes.

Create an authentication scheme **1-h** and set the authentication mode to local-HWTACACS, that is, the system performs the local authentication first and then the HWTACACS authentication. The HWTACACS authentication supersedes the local authentication when the level of a user is promoted.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme l-h
[Quidway-aaa-authen-l-h] authentication-mode hwtacacs local
[Quidway-aaa-authen-l-h] authentication-super hwtacacs super
[Quidway-aaa-authen-l-h] quit
```

Create an authorization scheme **hwtacacs**, and set the authorization mode to HWTACACS.

```
[Quidway-aaa] authorization-scheme hwtacacs
[Quidway-aaa-author-hwtacacs] authorization-mode hwtacacs
[Quidway-aaa-author-hwtacacs] quit
```

Create an accounting scheme **hwtacacs**, and set the accounting mode to HWTACACS.

```
[Quidway-aaa] accounting-scheme hwtacacs
[Quidway-aaa-accounting-hwtacacs] accounting-mode hwtacacs
[Quidway-aaa-accounting-hwtacacs] accounting start-fail online
```

Set the interval of interim accounting to 3 minutes.

```
[Quidway-aaa-accounting-hwtacacs] accounting realtime 3
[Quidway-aaa-accounting-hwtacacs] quit
```

Step 3 Create a domain Huawei and apply the authentication scheme 1-h, the HWTACACS authentication scheme, the HWTACACS accounting scheme, and the HWTACACS template of ht to the domain.

```
[Quidway-aaa] domain huawei
[Quidway-aaa-domain-huawei] authentication-scheme l-h
[Quidway-aaa-domain-huawei] authorization-scheme hwtacacs
[Quidway-aaa-domain-huawei] accounting-scheme hwtacacs
[Quidway-aaa-domain-huawei] hwtacacs-server ht
[Quidway-aaa-domain-huawei] quit
[Quidway-aaa] quit
```

Step 4 Verify the configuration.

Run the **display hwtacacs-server template** command on Switch B, and you can see that the configuration of the HWTACACS server template meets the requirements.

```
<Quidway> display hwtacacs-server template ht
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : ht
  Primary-authentication-server   : 129.7.66.66:49:-
  Primary-authorization-server    : 129.7.66.66:49:-
  Primary-accounting-server       : 129.7.66.66:49:-
  Secondary-authentication-server : 129.7.66.67:49:-
  Secondary-authorization-server  : 129.7.66.67:49:-
  Secondary-accounting-server     : 129.7.66.67:49:-
  Current-authentication-server   : 129.7.66.66:49:-
  Current-authorization-server    : 129.7.66.66:49:-
  Current-accounting-server       : 129.7.66.66:49:-
  Source-IP-address               : 0.0.0.0
  Shared-key                      : ****************
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Yes
  Traffic-unit                    : B
  ------------------------------------------------------------------------------
```

Run the **display domain** command on Switch B, and you can see that the configuration of the domain meets the requirements.

```
<Quidway> display domain name huawei

  Domain-name                    : huawei
  Domain-state                   : Active
  Authentication-scheme-name     : l-h
  Accounting-scheme-name         : hwtacacs
  Authorization-scheme-name      : hwtacacs
  Service-scheme-name            : -
  RADIUS-server-group            : -
  HWTACACS-server-template       : ht
```

----End

Configuration Files

```
#
sysname Quidway
#
hwtacacs-server template ht
 hwtacacs-server authentication 129.7.66.66
 hwtacacs-server authentication 129.7.66.67 secondary
 hwtacacs-server authorization 129.7.66.66
 hwtacacs-server authorization 129.7.66.67 secondary
 hwtacacs-server accounting 129.7.66.66
 hwtacacs-server accounting 129.7.66.67 secondary
 hwtacacs-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
#
aaa
 authentication-scheme default
 authentication-scheme l-h
  authentication-mode hwtacacs local
  authentication-super hwtacacs super
 authorization-scheme default
 authorization-scheme hwtacacs
  authorization-mode  hwtacacs
 accounting-scheme default
 accounting-scheme hwtacacs
  accounting-mode hwtacacs
  accounting start-fail online
  accounting realtime 3
 domain default
 domain default_admin
 domain huawei
  authentication-scheme l-h
  accounting-scheme hwtacacs
  authorization-scheme hwtacacs
  hwtacacs-server ht
#
return
```

6.2 NAC Configuration

This chapter describes the working principle and configuration of network access control (NAC).

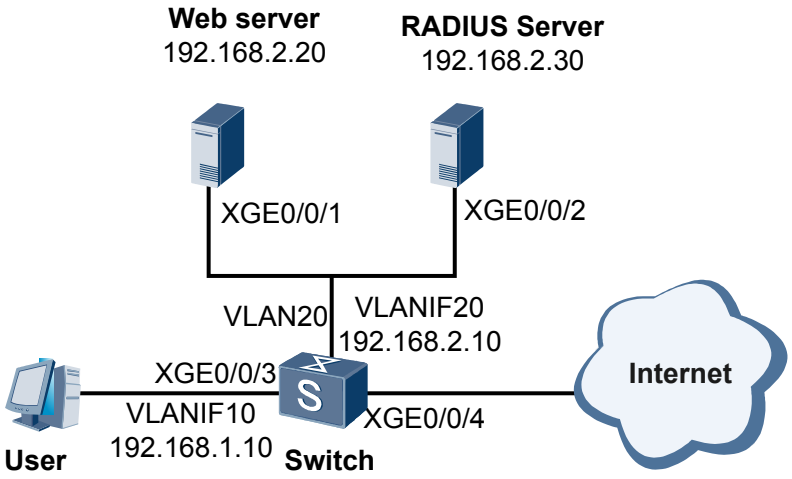
6.2.1 Example for Configuring Web Authentication

Networking Requirements

As shown in **Figure 6-3**, the requirements are as follows:

- The user interacts with the Web authentication server through the Switch.
- The authentication is performed by the RADIUS server.
- The user can access only the Web authentication server before authentication.
- After passing the Web authentication, the user can access the external network.

Figure 6-3 Network diagram for configuring Web authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Set the IP address of the Layer 3 interface connected to the user.
2. Configure a RADIUS server template.
3. Configure an AAA authentication template.
4. Configure a domain.
5. Configure the Web authentication function.

Data Preparation

To complete the configuration, you need the following data:

- IP address and URL of the Web authentication server
- IP address of the Layer 3 interface connected to the authentication terminal
- IP address and port number of the RADIUS authentication server
- Key of the RADIUS server (**hello**) and the retransmission count (2)
- Name of the AAA authentication scheme (**web1**)
- Name of the RADIUS server template (**rd1**)
- Name of the user domain (**isp1**)

NOTE

In this example, only the configuration of the Switch is provided, and the configurations of the Web server and RADIUS server are omitted.

Procedure

Step 1 Set the IP address of the Layer 3 interface connected to the user.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface xgigabitethernet 0/0/3
```

```
[Quidway-XGigabitEthernet0/0/3] port link-type access
[Quidway-XGigabitEthernet0/0/3] port default vlan 10
[Quidway-XGigabitEthernet0/0/3] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 192.168.1.10 24
[Quidway-Vlanif10] quit
```

Step 2 Configure a RADIUS server template.

Configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
```

Set the IP address and port number of the primary RADIUS authentication server.

```
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
```

Set the key and retransmission count of the RADIUS server.

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Step 3 Create an authentication scheme **web1** and set the authentication method to RADIUS authentication.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

Step 4 Create a domain **isp1** and bind the authentication scheme and RADIUS server template to the domain.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
```

Step 5 Configure the Web authentication function.

Set the IP address and URL of the Web authentication server

```
[Quidway] web-auth-serer isp1
[Quidway-web-auth-server-isp1] server-ip 192.168.2.20
[Quidway-web-auth-server-isp1] url http://www.isp1.com
```

Bind the Web authentication server to the Layer 3 interface.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] web-auth-server isp1
[Quidway-Vlanif10] quit
```

Configure a free rule to redirect the user to the Web authentication page when the user starts the Web browser.

```
[Quidway] portal free-rule 20 destination ip 192.168.2.20 mask 24  source any
```

Step 6 Verify the configuration.

Run the **display web-auth-server configuration** command on the Switch, and you can view the configuration of the Web authentication server.

```
<Quidway> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
  ------------------------------------------------------------------------------
  Web-auth-server Name : isp1
  IP-address           : 192.168.1.20
  Shared-key           : huawei
```

```
  Port / PortFlag      : 50100 / NO
  URL                  : www.isp1.com
   ------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

----End

Configuration Files

```
#
sysname Quidway
#
vlan batch 10
#
web-auth-server isp1
 server-ip 10.1.1.1
 port 50100
 url http//www.isp1.com
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  radius-server  rd1
#
interface Vlanif10
 ip address 192.168.1.10 255.255.255.0
 web-auth-server web
#
interface XGigabitEthernet0/0/3
 port link-type access
 port default vlan 10
#
return
```

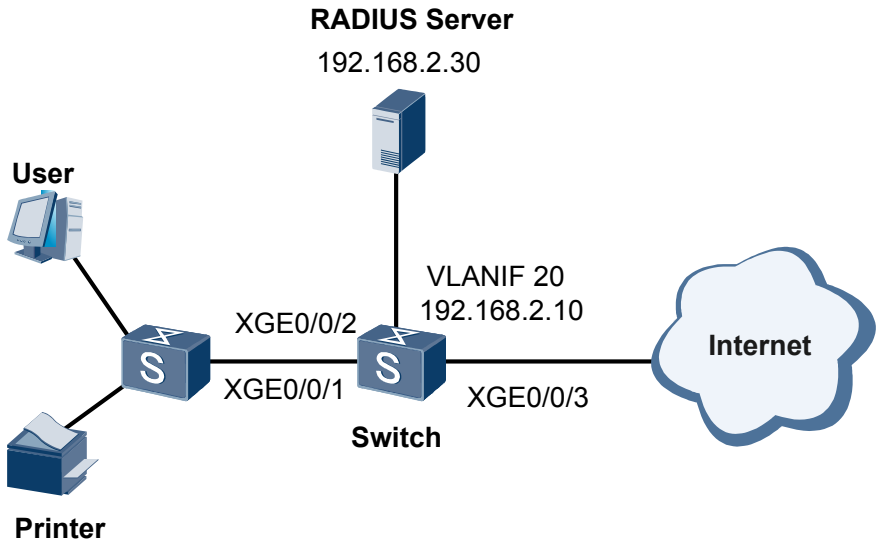
6.2.2 Example for Configuring 802.1x Authentication

Networking Requirements

As shown in **Figure 6-4**, the requirements are as follows:

- 802.1x authentication is performed for the user connected to XGE 0/0/1 to control the user's access to the Internet. The default access control mode is adopted, that is, the Switch controls access of the user based on the MAC address of the user.
- The authentication is performed by the RADIUS server.
- The maximum number of users on XGE 0/0/1 is 100.
- MAC address bypass authentication is performed for the printer connected to XGE 0/0/1.

Figure 6-4 Networking diagram for configuring 802.1x authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a RADIUS server template.
2. Configure an AAA authentication template.
3. Configure a domain.
4. Configure the 802.1x authentication function.

Data Preparation

To complete the configuration, you need the following data:

- IP address and port number of the RADIUS authentication server
- Key of the RADIUS server (**hello**) and the retransmission count (2)
- Name of the AAA authentication scheme (**web1**)
- Name of the RADIUS server template (**rd1**)
- Name of the user domain (**isp1**)

NOTE

In this example, only the configuration of the Switch is provided, and the configuration of RADIUS server is omitted.

Procedure

Step 1 Configure a RADIUS server template.

Configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
```

Set the IP address and port number of the primary RADIUS authentication server.

```
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
```

Set the key and retransmission count of the RADIUS server.

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Step 2 Create an authentication scheme **web1** and set the authentication method to RADIUS authentication.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

Step 3 Create a domain **isp1** and bind the authentication scheme and RADIUS server template to the domain.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
```

Step 4 Configure the 802.1x authentication function.

Enable 802.1x authentication globally and on XGE 0/0/1.

```
[Quidway] dot1x enable
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dot1x enable
```

Set the maximum number of access users on XGE 0/0/1.

```
[Quidway-XGigabitEthernet0/0/1] dot1x max-user 100
```

Configure MAC address bypass authentication.

```
[Quidway-XGigabitEthernet0/0/1] dot1x mac-bypass
```

Step 5 Verify the configuration.

Run the **display dot1x interface** command on the Switch, and you can view the configuration and statistics of 802.1x authentication.

```
<Quidway> display dot1x interface xgigabitethernet 0/0/1
 XGigabitEthernet0/0/1 status: UP  802.1x protocol is Enabled[mac-
bypass]
  Port control type is Auto
  Authentication method is MAC-based
  Reauthentication is disabled
  Maximum users: 100
  Current users: 1

  Authentication Success: 4          Failure: 0
  EAPOL Packets: TX     : 8          RX     : 16
  Sent      EAPOL Request/Identity Packets  : 4
            EAPOL Request/Challenge Packets : 4
            Multicast Trigger Packets       : 0
            EAPOL Success Packets           : 4
            EAPOL Failure Packets           : 0
  Received  EAPOL Start Packets             : 4
            EAPOL LogOff Packets            : 3
            EAPOL Response/Identity Packets : 4
            EAPOL Response/Challenge Packets: 4
```

----End

Configuration Files

```
#
```

```
sysname Quidway
#
dot1x enable
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  radius-server rd1
#
interface XGigabitEthernet0/0/1
 dot1x mac-bypass
 dot1x max-user 100
#
return
```

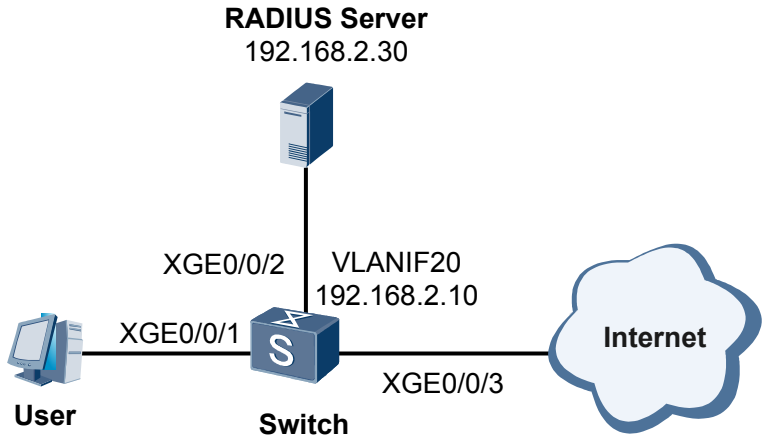
6.2.3 Example for Configuring MAC Address Authentication

Networking Requirements

As shown in **Figure 6-5**, the requirements are as follows:

- Authentication is performed for the user connected to XGE 0/0/1 to control the users access to the Internet.
- The authentication is performed by the RADIUS server.
- The default authentication method is used, that is, the MAC address without hyphens is used as the user name in authentication.
- The maximum number of users on XGE 0/0/1 is 100.

Figure 6-5 Networking diagram for configuring MAC address authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a RADIUS server template.
2. Configure an AAA authentication template.
3. Configure the domain of the users that use MAC address authentication.
4. Configure the MAC address authentication.

Data Preparation

To complete the configuration, you need the following data:

- IP address and port number of the RADIUS authentication server
- Key of the RADIUS server (**hello**) and the retransmission count (2)
- Name of the AAA authentication scheme (**web1**)
- Name of the RADIUS server template (**rd1**)
- Name of the user domain (**isp1**)

NOTE

In this example, only the configuration of the Switch is provided, and the configuration of RADIUS server is omitted.

Procedure

Step 1 Configure a RADIUS server template.

Configure a RADIUS server template **rd1**.

```
[Quidway] radius-server template rd1
```

Set the IP address and port number of the primary RADIUS authentication server.

```
[Quidway-radius-rd1] radius-server authentication 192.168.2.30 1812
```

Set the key and retransmission count of the RADIUS server.

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] radius-server retransmit 2
[Quidway-radius-rd1] quit
```

Step 2 Create an authentication scheme **web1** and set the authentication method to RADIUS authentication.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

Step 3 Create a domain **isp1** and bind the authentication scheme and RADIUS server template to the domain.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
```

Step 4 Configure the MAC address authentication function.

Enable MAC address authentication globally and on XGE 0/0/1.

```
[Quidway] mac-authen
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] mac-authen
```

Set the maximum number of access users on XGE 0/0/1.

```
[Quidway-XGigabitEthernet0/0/1] mac-authen max-user 100
[Quidway-XGigabitEthernet0/0/1] quit
```

Specify domain **isp1** as the domain of the users that use MAC address authentication.

```
[Quidway] mac-authen domain isp1
```

Step 5 Verify the configuration.

Run the **display mac-authen interface** command on the Switch, and you can view the configuration of MAC address authentication.

```
<Quidway> display mac-authen interface xgigabitethernet 0/0/1
  XGigabitEthernet0/0/1 state: UP  MAC address authentication is enabled
  Maximum users: 100
  Current users: 2
  Guest VLAN is disabled
```

----End

Configuration Files

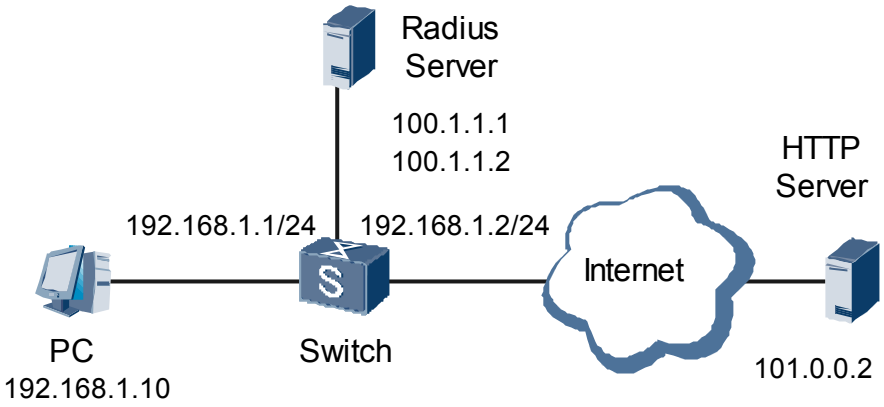
```
#
sysname Quidway
#
mac-authen
mac-authen domain isp1
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  radius-server rd1
#
interface XGigabitEthernet0/0/1
 mac-authen
 mac-authen max-user 100
#
return
```

6.2.4 Example for Configuring the RADIUS Server to Deliver Authorization ACL

Networking Requirements

As shown in **Figure 6-6**, the PC accesses the network using 802.1x authentication. The authentication server is a RADIUS server. An HTTP server is located on the Internet. After the user goes online, the RADIUS server is required to deliver ACL. The user then is allowed to connect to the Internet, but cannot access the HTTP server.

Figure 6-6 Networking diagram for configuring 802.1x authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the RADIUS authentication server to deliver the authorization ACL.
2. Configure a RADIUS server template.
3. Configure an AAA authentication template.
4. Configure a domain.
5. Configure an ACL, which is the same as the ACL on the RADIUS server, on the Switch and configure the ACL rules.
6. Configure 802.1x authentication.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the RADIUS authentication server: 100.1.1.1; authentication port number: 1812
- RADIUS server template: rd1
- Shared key of the RADIUS server: hello
- AAA authentication scheme: web1
- Domain: isp1
- ACL number: 3000

NOTE

In this example, only the configuration of the Switch is provided, and the configuration of RADIUS server is not mentioned here.

Procedure

Step 1 Configure a RADIUS server template.

Configure a RADIUS server template rd1.

```
[Quidway] radius-server template rd1
```

Configure the IP address and port number of the primary RADIUS authentication server.

```
[Quidway-radius-rd1] radius-server authentication 100.1.1.1 1812
```

Configure the shared key of the RADIUS server.

```
[Quidway-radius-rd1] radius-server shared-key cipher hello
[Quidway-radius-rd1] quit
```

Step 2 Create an authentication scheme web1 and set the authentication method to RADIUS authentication.

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme web1
[Quidway-aaa-authen-1] authentication-mode radius
[Quidway-aaa-authen-1] quit
```

Step 3 Create a domain isp1 and bind the authentication scheme and RADIUS server template to the domain.

```
[Quidway-aaa] domain isp1
[Quidway-aaa-domain-isp1] authentication-scheme web1
[Quidway-aaa-domain-isp1] accounting-scheme web1
[Quidway-aaa-domain-isp1] radius-server rd1
[Quidway-aaa-domain-isp1] quit
[Quidway-aaa] quit
```

Step 4 Configure ACL 3000 to reject the packets with the destination address 101.0.0.2.

```
[Quidway] acl 3000
[Quidway-acl-adv-3000] rule 0 deny ip destination 101.0.0.2 0
[Quidway-acl-adv-3000] quit
```

Step 5 Configure the 802.1x authentication.

Enable the 802.1x authentication globally.

```
[Quidway] dot1x enable
```

Step 6 Verify the configuration.

After the user goes online successfully, ping the HTTP server from the PC to check whether ACL 3000 takes effect.

```
[Quidway] ping 101.0.0.2
PING 101.0.0.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- 10.0.0.1 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

----End

Configuration Files

```
#
sysname Quidway
#
dot1x enable
#
radius-server template rd1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 10.1.1.1 1812
 radius-server accounting 100.1.1.2 1813
#
```

```
acl number 3000
 rule 0 deny ip destination 101.0.0.2 0
#
aaa
 authentication-scheme web1
  authentication-mode radius
 domain isp1
  authentication-scheme web1
  accounting-scheme web1
  radius-server rd1
#
return
```

6.3 DHCP Snooping Configuration

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on the S6700 to defend against DHCP attacks.

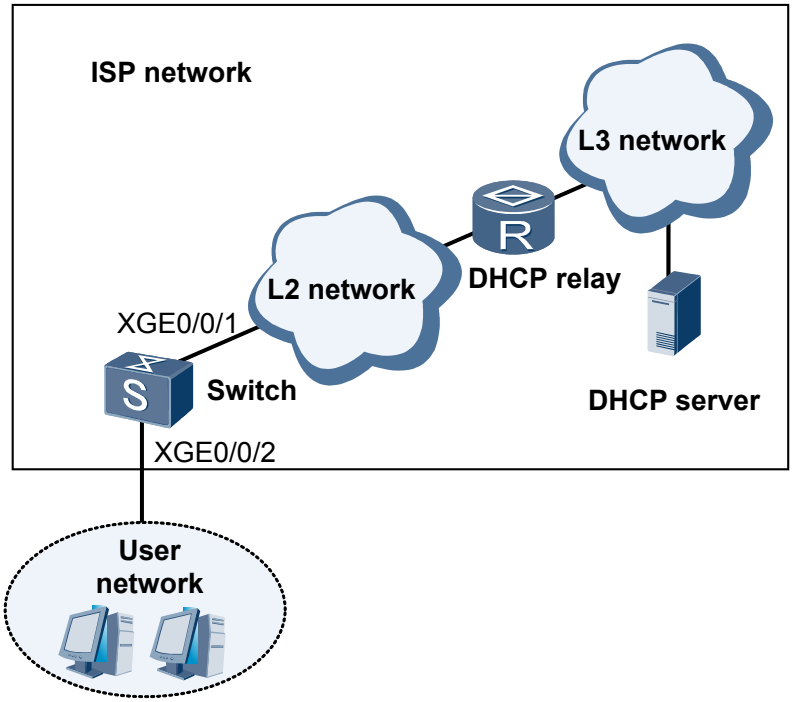
6.3.1 Example for Preventing Bogus DHCP Server Attacks

This section describes the configuration of preventing bogus DHCP server attacks, including the configuration of the trusted interface and the alarm function for discarded DHCP Reply packets.

Networking Requirements

As shown in **Figure 6-7**, the Switch is deployed between the user network and the Layer 2 network of the ISP. To prevent bogus DHCP server attacks, it is required that DHCP snooping be configured on the Switch, the user-side interface be configured as an untrusted interface, the network-side interface be configured as the trusted interface, and the alarm function for discarded DHCP Reply packets be configured.

Figure 6-7 Networking diagram for preventing bogus DHCP server attacks



Configuration Roadmap

The configuration roadmap is as follows: (Assume that the DHCP server has been configured.)

1. Enable DHCP snooping globally and on the interface.
2. Enable bogus DHCP server detection.
3. Configure the interface connected to the DHCP server as the trusted interface.
4. Configure the alarm function for discarded DHCP Reply packets.

Data Preparation

To complete the configuration, you need the following data:

- XGE 0/0/1 being the trusted interface and XGE 0/0/2 being the untrusted interface
- Alarm threshold being 120

NOTE

This configuration example provides only the commands related to the DHCP snooping configuration.

Procedure

Step 1 Enable DHCP snooping.

Enable DHCP snooping globally.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

Enable bogus DHCP server detection.

```
[Quidway] dhcp server detect
```

Enable DHCP snooping on the user-side interface.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] dhcp snooping enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 Configure the interface as the trusted interface or an untrusted interface.

Configure the interface on the DHCP server side as the trusted interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-XGigabitEthernet0/0/1] quit
```

Configure the user-side interface as an untrusted interface.

After DHCP snooping is enabled on XGE 0/0/2, XGE 0/0/2 is an untrusted interface by default.

Step 3 Configure the alarm function for discarded DHCP Reply packets.

Configure the Switch to discard the Reply messages received by untrusted interfaces, and set the alarm threshold.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] dhcp snooping alarm dhcp-reply enable threshold
```

```
120
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 4 Verify the configuration.

Run the **display dhcp snooping global** command on the Switch, and you can view that DHCP snooping is enabled globally and in the interface view.

```
<Quidway> display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at vlan :NULL

 Dhcp snooping enable is configured at interface :
 XGigabitEthernet0/0/2

 Dhcp snooping trusted is configured at interface :
 XGigabitEthernet0/0/1

 Dhcp option82 insert is configured at interface :NULL

 Dhcp option82 rebuild is configured at interface :NULL

 Dhcp option82 insert is configured at vlan :NULL

 Dhcp option82 rebuild is configured at vlan :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 60


<Quidway> display dhcp snooping interface xgigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0

<Quidway> display dhcp snooping interface xgigabitethernet 0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp packet dropped by untrust-reply checking = 10
```

----End

Configuration Files

```
#
 dhcp enable
 dhcp snooping enable
 dhcp server detect
#
interface XGigabitEthernet0/0/1
 dhcp snooping trusted
#
interface XGigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
#
return
```

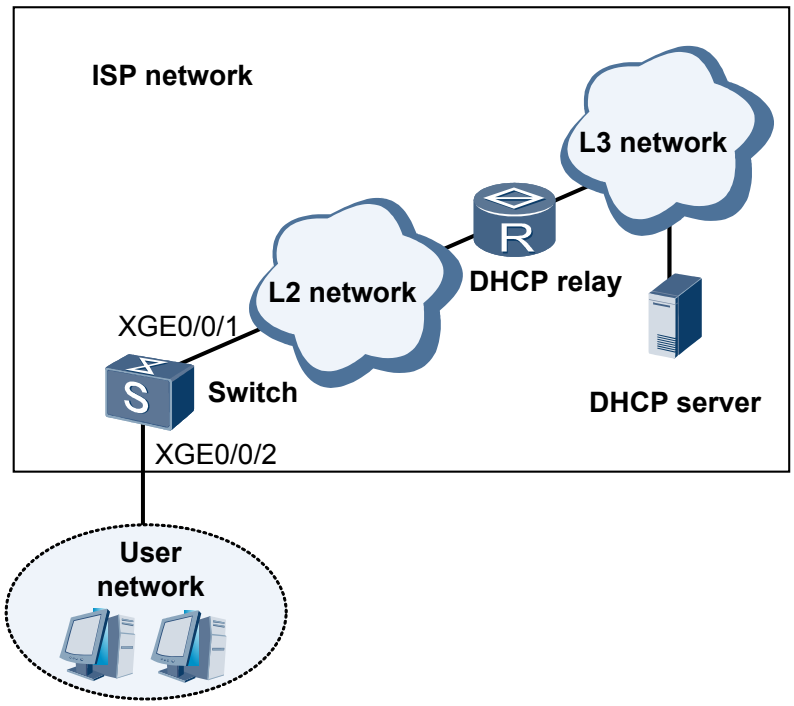
6.3.2 Example for Preventing DoS Attacks by Changing the CHADDR Field

This section describes the configuration of preventing DoS attacks by changing the CHADDR field, including the configuration of the function of checking the CHADDR field of DHCP Request messages on the user-side interface and the alarm function for discarded packets.

Networking Requirements

As shown in **Figure 6-8**, the Switch is deployed between the user network and the ISP Layer 2 network. To prevent DoS attacks by changing the CHADDR field, it is required that DHCP snooping be configured on the Switch. The CHADDR field of DHCP Request messages is checked. If the CHADDR field of DHCP Request messages matches the source MAC address in the frame header, the messages are forwarded. Otherwise, the messages are discarded. The alarm function for discarded packets is configured.

Figure 6-8 Networking diagram for preventing DoS attacks by changing the CHADDR field



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping globally and on the interface.
2. Configure the interface connected to the DHCP server as the trusted interface.
3. Enable the function of checking the CHADDR field of DHCP Request messages on the user-side interface.
4. Configure the alarm function for discarded packets.

Data Preparation

To complete the configuration, you need the following data:

- Alarm threshold

NOTE

This configuration example provides only the commands related to the DHCP snooping configuration.

Procedure

Step 1 Enable DHCP snooping.

Enable DHCP snooping globally.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

Enable DHCP snooping on the user-side interface.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] dhcp snooping enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 Configure the interface as the trusted interface or an untrusted interface.

Configure the interface on the DHCP server side as the trusted interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-XGigabitEthernet0/0/1] quit
```

Configure the user-side interface as an untrusted interface.

After DHCP snooping is enabled on XGE 0/0/2, XGE 0/0/2 is an untrusted interface by default.

Step 3 Enable the function of checking the CHADDR field of DHCP Request messages on the user-side interface, and configure the alarm function and threshold for discarded packets..

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
```

Step 4 Verify the configuration.

Run the **display dhcp snooping** command on the Switch, and you can view that DHCP snooping is enabled globally and in the interface view.

```
<Quidway> display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at vlan :NULL

 Dhcp snooping enable is configured at interface :
 XGigabitEthernet0/0/2

 Dhcp snooping trusted is configured at interface :
 XGigabitEthernet0/0/1

 Dhcp option82 insert is configured at interface :NULL

 Dhcp option82 rebuild is configured at interface :NULL

 Dhcp option82 insert is configured at vlan :NULL

 Dhcp option82 rebuild is configured at vlan :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 25

<Quidway> display dhcp snooping interface xgigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0
<Quidway> display dhcp snooping interface xgigabitethernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp packet dropped by dhcp-chaddr checking = 25
```

```
 dhcp packet dropped by untrust-reply checking = 0
```

----End

Configuration Files

```
#
 dhcp enable
 dhcp snooping enable
#
interface XGigabitEthernet0/0/1
 dhcp snooping trusted
#
interface XGigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
#
return
```

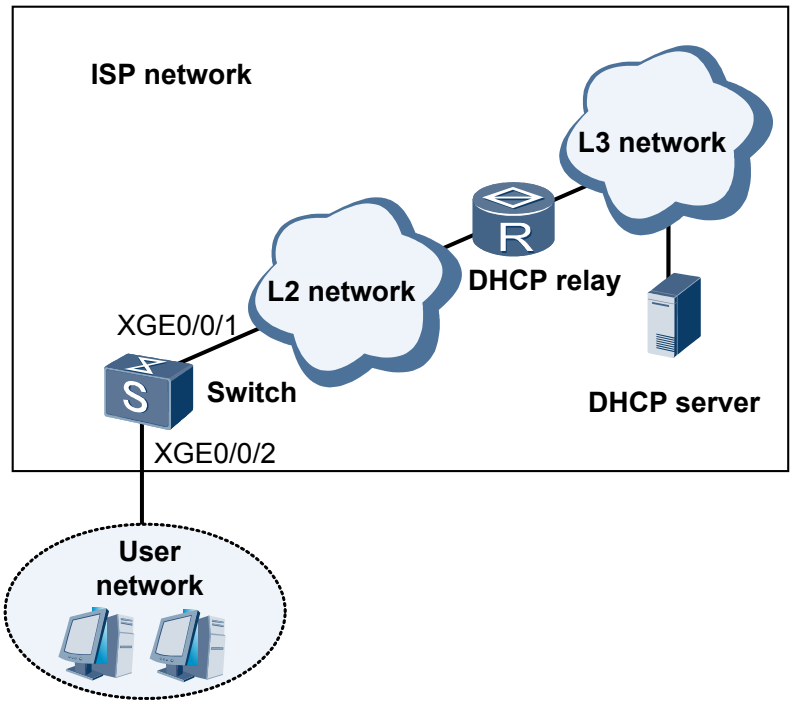
6.3.3 Example for Preventing Attackers from Sending Bogus DHCP Messages for Extending IP Address Leases

This section describes the configuration of preventing attackers from sending bogus DHCP messages for extending IP address leases, including the configuration of the function of checking the DHCP Request messages on the user-side interface and the alarm function for discarded packets.

Networking Requirements

As shown in **Figure 6-9**, the Switch is deployed between the user network and the ISP Layer 2 network. To prevent attackers from sending bogus DHCP messages for extending IP address leases, it is required that DHCP snooping be configured on the Switch and the DHCP snooping binding table be created. If the received DHCP Request messages match entries in the binding table, they are forwarded; otherwise, they are discarded. The alarm function for discarded packets is configured.

Figure 6-9 Networking diagram for preventing attackers from sending bogus DHCP messages for extending IP address leases



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping globally and on the interface.
2. Configure the interface connected to the DHCP server as the trusted interface.
3. Use the operation mode of the DHCP snooping binding table to check DHCP Request messages.
4. Configure the alarm function for discarded packets.

Data Preparation

To complete the configuration, you need the following data:

- ID of the VLAN that each interface belongs to
- Static IP addresses from which packets are forwarded
- Alarm threshold

NOTE

This configuration example provides only the commands related to the DHCP snooping configuration.

Procedure

Step 1 Enable DHCP snooping.

Enable DHCP snooping globally.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

Enable DHCP snooping on the user-side interface.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] dhcp snooping enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 Configure the interface as the trusted interface or an untrusted interface.

Configure the interface on the DHCP server side as the trusted interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-XGigabitEthernet0/0/1] quit
```

Configure the user-side interface as an untrusted interface.

After DHCP snooping is enabled on XGE 0/0/2, XGE 0/0/2 is an untrusted interface by default.

Step 3 Configure the function of checking DHCP Request messages and the alarm function for discarded packets.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] dhcp snooping check dhcp-request enable alarm dhcp-request enable threshold 120
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 4 Check the DHCP snooping binding entries.

Run the **display dhcp snooping user-bind all** command, and you can view all the DHCP snooping binding entries of users.

```
<Quidway> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
-------------------------------------------------------------------------------
10.1.1.3        0000-005e-008a   3 /--  /--      XGE0/0/2        2010.08.14-12:58
-------------------------------------------------------------------------------
print count:           1         total count:           1
```

Step 5 Verify the configuration.

Run the **display dhcp snooping global** command on the Switch, and you can view that DHCP snooping is enabled globally and on the interface.

```
<Quidway> display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at vlan :NULL

 Dhcp snooping enable is configured at interface :
 XGigabitEthernet0/0/2

 Dhcp snooping trusted is configured at interface :NULL
 XGigabitEthernet0/0/1
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 45

<Quidway> display dhcp snooping interface xgigabitethernet 0/0/1
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0
<Quidway> display dhcp snooping interface xgigabitethernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable alarm dhcp-request threshold 120
```

```
 dhcp packet dropped by dhcp-request checking = 45
 dhcp packet dropped by untrust-reply checking = 0
```

----End

Configuration Files

```
#
 dhcp enable
 dhcp snooping enable
#
interface XGigabitEthernet0/0/1
 dhcp snooping trusted
#
interface XGigabitEthernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable alarm dhcp-request threshold 120
#
return
```

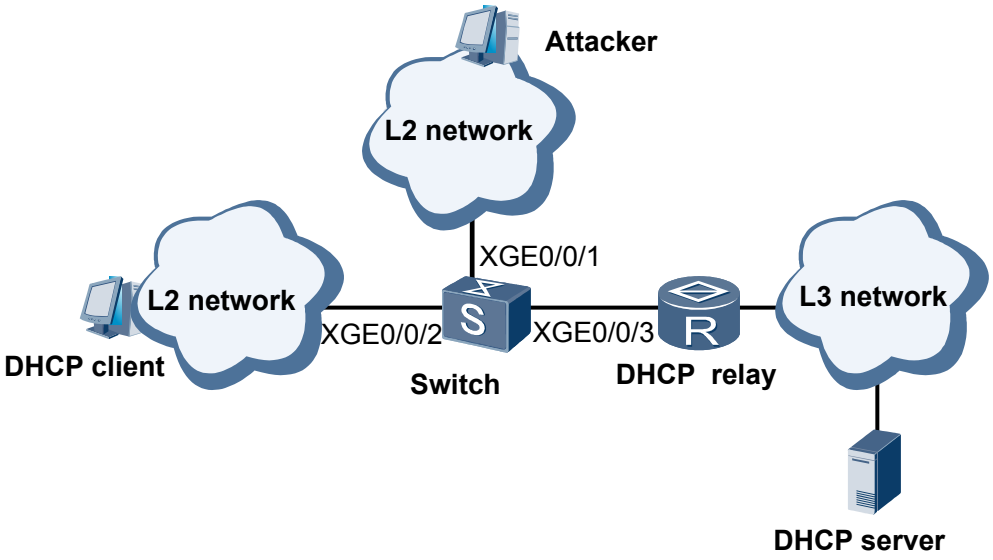
6.3.4 Example for Limiting the Rate of Sending DHCP Messages

This section describes the configuration of limiting the rate of sending DHCP messages, including the configuration of the rate of sending DHCP messages to the protocol stack and the alarm function for discarded packets.

Networking Requirements

As shown in **Figure 6-10**, to prevent the attacker from sending a large number of DHCP Request messages, it is required that DHCP snooping be enabled on the Switch to control the rate of sending DHCP Request messages to the protocol stack. At the same time, the alarm function for discarded packets needs to be enabled.

Figure 6-10 Networking diagram for limiting the rate of sending DHCP messages



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping globally and in the interface view.
2. Configure the interface connected to the DHCP server as the trusted interface.
3. Set the rate of sending DHCP Request messages to the protocol stack on interfaces.
4. Configure the alarm function for discarded packets on interfaces.

Data Preparation

To complete the configuration, you need the following data:

- Rate of sending DHCP Request messages
- Alarm threshold

NOTE

This configuration example provides only the commands related to the DHCP snooping configuration.

Procedure

Step 1 Enable DHCP snooping.

Enable DHCP snooping globally.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

Enable DHCP snooping on the user-side interface. The configuration procedures of XGE 0/0/2 and XGE0/0/3 are similar to the configuration procedure of XGE 0/0/1, and is not mentioned here.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping enable
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Configure the interface as the trusted interface or an untrusted interface.

Configure the interface on the DHCP server side as the trusted interface.

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] dhcp snooping trusted
[Quidway-XGigabitEthernet0/0/3] quit
```

Configure the user-side interface as an untrusted interface.

After DHCP snooping is enabled on XGE 0/0/1 and XGE 0/0/2, XGE 0/0/1 and XGE 0/0/2 is an untrusted interface by default.

Step 3 Configure the rate of sending DHCP messages to the DHCP protocol stack and the alarm function for discarded packets.

Configure the rate of sending DHCP messages to the DHCP protocol stack and the alarm function for discarded packets on interfaces. The configuration procedures of XGE 0/0/2 andXGE0/0/3 are similar to the configuration procedure of XGE 0/0/1, and is not mentioned here.

```
[Quidway-XGigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable 50 alarm dhcp-
rate enable threshold 50
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 4 Verify the configuration.

Run the **display dhcp snooping global** command on the Switch, and you can view that DHCP snooping is enabled globally or in interface view.

```
[Quidway] display dhcp snooping global
 dhcp snooping enable

 Dhcp snooping enable is configured at these vlan :NULL

 Dhcp snooping enable is configured at these interface :
 XGigabitEthernet0/0/1 XGigabitEthernet0/0/2 XGigabitEthernet0/0/3

 Dhcp snooping trusted is configured at these interface :
 XGigabitEthernet0/0/3
 Dhcp option82 insert is configured at these interface :NULL

 Dhcp option82 rebuild is configured at these interface :NULL

 Dhcp option82 insert is configured at these vlan :NULL

 Dhcp option82 rebuild is configured at these vlan :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
```

Run the **display dhcp snooping interface** command on the Switch, and you can view the configuration of DHCP snooping in interface view.

```
[Quidway] display dhcp snooping interface xgigabitethernet0/0/3
 dhcp snooping trusted
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
 dhcp packet dropped by untrust-reply checking = 0
[Quidway] display dhcp snooping interface xgigabitethernet 0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
 dhcp packet dropped by untrust-reply checking = 0
[Quidway] display dhcp snooping interface XGigabitEthernet 0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
 dhcp packet dropped by untrust-reply checking = 0
```

----End

Configuration Files

```
#
 dhcp enable
 dhcp snooping enable
#
interface xgigabitethernet0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
#
interface xgigabitethernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
#
interface XGigabitEthernet0/0/3
 dhcp snooping enable
 dhcp snooping trusted
 dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
#
return
```

6.3.5 Example for Applying DHCP Snooping on a Layer 2 Network

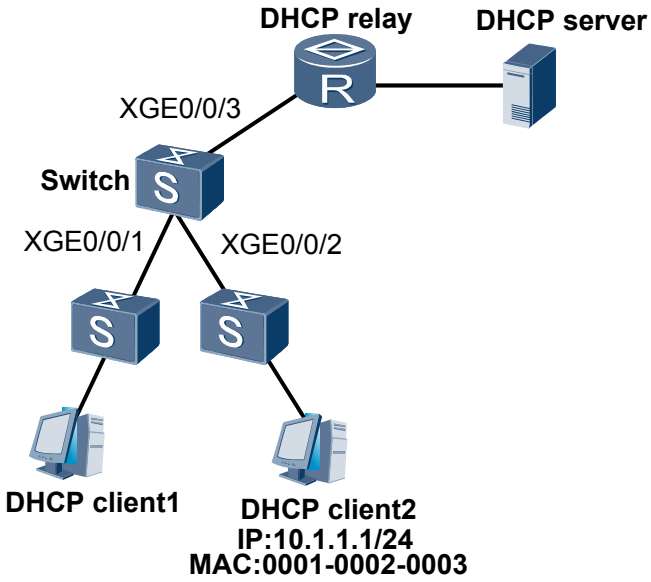
This section describes the configuration of DHCP snooping on a Layer 2 network, including the configuration of the trusted interface, the function of checking DHCP messages, the function of limiting the rate of sending DHCP messages, and the Option 82 function.

Networking Requirements

As shown in **Figure 6-11**, DHCP clients are connected to the Switch through VLAN 10. DHCP client1 uses the dynamically allocated IP address and DHCP client2 uses the statically configured IP address. It is required that DHCP snooping be configured on user-side interfaces XGE 0/0/1 and XGE 0/0/2 of the Switch to prevent the following type of attacks:

- Bogus DHCP server attacks
- DoS attacks by changing the value of the CHADDR field
- Attacks by sending bogus messages to extend IP address leases
- Attacks by sending a large number of DHCP Request messages

Figure 6-11 Networking diagram for configuring DHCP snooping



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping globally and in the interface view.
2. Configure interfaces to be trusted or untrusted to prevent bogus DHCP server attacks.
3. Configure the DHCP snooping binding table and check DHCP Request messages by matching them with entries in the binding table to prevent attackers from sending bogus DHCP messages for extending IP address leases.
4. Configure the function of checking the CHADDR field in DHCP Request messages to prevent attackers from changing the CHADDR field in DHCP Request messages.

5. Set the rate of sending DHCP Request messages to the protocol stack to prevent attackers from sending a large number of DHCP Request messages.
6. Configure the Option 82 function.
7. Configure the alarm function for discarded packets.

Data Preparation

To complete the configuration, you need the following data:

- VLAN that the interface belongs to being 10
- XGE 0/0/1 and XGE0/0/2 being untrusted interfaces and XGE 0/0/3 being the trusted interface
- Static IP address from which packets are forwarded being 10.1.1.1/24 and corresponding MAC address being 0001-0002-0003
- Rate of sending DHCP messages to the protocol stack being 90
- Mode of the Option 82 function being **insert**
- Alarm threshold of the number of discarded packets being 120

NOTE

This configuration example provides only the commands related to the DHCP snooping configuration.

Procedure

Step 1 Enable DHCP snooping.

Enable DHCP snooping globally.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

Enable DHCP snooping on the interface at the user side. The configuration procedure of XGE 0/0/2 is the same as the configuration procedure of XGE 0/0/1, and is not mentioned here.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping enable
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 2 Configure the interface as trusted.

Configure the interface connecting to the DHCP server as the trusted interface and enable DHCP snooping on all the interfaces connecting to the DHCP client. If the interface on the client side is not configured as trusted, the default mode of the interface is untrusted after DHCP snooping is enabled on the interface. This prevents bogus DHCP server attacks.

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] dhcp snooping trusted
[Quidway-XGigabitEthernet0/0/3] quit
```

Step 3 Configure the checking for certain types of packets and alarm function.

Enable the checking of DHCP Request messages and alarm function on the interfaces on the DHCP client side to prevent attackers from sending bogus DHCP messages for extending IP address leases. The configuration of XGE 0/0/2 is the same as the configuration of XGE 0/0/1, and is not mentioned here.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping check dhcp-request enable alarm dhcp-request enable threshold 120
```

Enable the checking of the CHADDR field and alarm function on the interfaces on the DHCP client side to prevent attackers from changing the CHADDR field in DHCP Request messages. The configuration of XGE 0/0/2 is the same as the configuration of XGE 0/0/1, and is not mentioned here.

```
[Quidway-XGigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 4 Check the DHCP snooping binding entries.

Run the **display dhcp snooping user-bind all** command, and you can view the DHCP snooping binding entries of users.

```
<Quidway> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
-------------------------------------------------------------------------------
10.1.1.1        0001-0002-0003   10 /--  /--     XGE0/0/2        2010.08.14-12:58
-------------------------------------------------------------------------------
print count:           1         total count:           1
```

Step 5 Limit the rate of sending DHCP messages.

Check the rate of sending DHCP messages to prevent attackers from sending DHCP Request messages.

```
[Quidway] dhcp snooping check dhcp-rate enable
[Quidway] dhcp snooping check dhcp-rate 90
```

Step 6 Configure the Option 82 function.

Configure the user-side interface to append the Option 82 field to DHCP messages. The configuration of XGE 0/0/2 is the same as the configuration of XGE 0/0/1, and is not mentioned here.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp option82 insert enable
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 7 Configure the alarm function for discarded packets.

Enable the alarm function for discarded DHCP Reply packets, and set the alarm threshold of the number of discarded packets. The configuration of XGE 0/0/2 is similar to the configuration of XGE 0/0/1, and is not mentioned here.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] dhcp snooping alarm dhcp-reply enable threshold 120
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 8 Verify the configuration.

Run the **display dhcp snooping global** command on the Switch, and you can view that DHCP snooping is enabled globally. You can also view the statistics on alarms.

```
[Quidway] display dhcp snooping global
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 90

 Dhcp snooping enable is configured at these vlan :NULL
```

```
 Dhcp snooping enable is configured at these interface :
 XGigabitEthernet0/0/1 XGigabitEthernet0/0/2

 Dhcp snooping trusted is configured at these interface :
 XGigabitEthernet0/0/3

 Dhcp option82 insert is configured at these interface :
 XGigabitEthernet0/0/1 XGigabitEthernet0/0/2

 Dhcp option82 rebuild is configured at these interface :NULL

 dhcp packet drop count within alarm range : 0
 dhcp packet drop count total : 0
```

Run the **display dhcp snooping interface** command, and you can view information about DHCP snooping on the interface.

```
[Quidway] display dhcp snooping interface XGigabitEthernet 0/0/1
 dhcp snooping enable
 dhcp option82 insert enable
 dhcp snooping check dhcp-request enable alarm dhcp-request threshold 120
 dhcp packet dropped by dhcp-request checking = 0
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp packet dropped by dhcp-chaddr checking = 0
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp packet dropped by untrust-reply checking = 0

[Quidway] display dhcp snooping interface xgigabitethernet 0/0/3
 dhcp snooping trusted
 dhcp packet dropped by untrust-reply checking = 0
```

Run the **display dhcp static user-bind all** command, and you can view all the DHCP static binding entries of users.

```
<Quidway> display dhcp static user-bind all
DHCP static Bind-table::
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.1.1        0001-0002-0003   10 /--  /--     XGE0/0/2        2010.08.14-12:58
--------------------------------------------------------------------------------
print count:           1         total count:           1
```

Run the **display dhcp option82 interface** command, and you can view the configuration of Option 82 on the interface.

```
[Quidway] display dhcp option82 interface XGigabitEthernet 0/0/1
 dhcp option82 insert enable
```

----End

Configuration Files

```
#
 dhcp enable
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 90
#
 user-bind static ip-address 10.1.1.1 mac-address 0001-0002-0003 interface
XGigabitEthernet 0/0/2 vlan 10
#
interface XGigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp snooping check dhcp-request enable alarm dhcp-request enable threshold 120

 dhcp option82 insert enable
```

```
#
interface XGigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable alarm dhcp-chaddr enable threshold 120
 dhcp snooping check dhcp-request enable alarm dhcp-request enable threshold 120

 dhcp option82 insert enable
#
interface XGigabitEthernet0/0/3
 dhcp snooping trusted
#
return
```

6.4 ARP Security Configuration

The ARP security technology ensures security and robustness of network devices by filtering out untrusted ARP packets and perform timestamp suppression for some ARP packets.

6.4.1 Example for Configuring ARP Security Functions

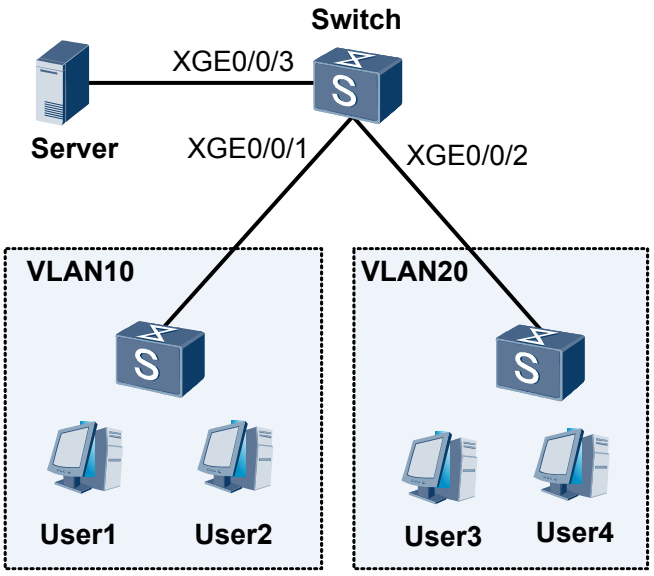
Networking Requirements

As shown in **Figure 6-12**, the Switch is connected to a server through XGE 0/0/3 and is connected to four users in VLAN 10 and VLAN 20 through XGE 0/0/1 and XGE 0/0/2. There are the following ARP attacks on the network:

- The server may send several packets with an unreachable destination IP address, and the number of these packets is larger than the number of packets from common users.
- After virus attacks occur on User 1, a large number of ARP packets are sent. Among these packets, the source IP address of certain ARP packets changes on the local network segment and the source IP address of certain ARP packets is the same as the IP address of the gateway.
- User 3 constructs a large number of ARP packets with a fixed IP address to attack the network.
- User 4 constructs a large number of ARP packets with an unreachable destination IP address to attack the network.

It is required that ARP security functions be configured on the Switch to prevent the preceding attacks. The suppression rate of ARP Miss packets set on the server should be greater than the suppression rate of other users.

Figure 6-12 Networking diagram for configuring ARP security functions



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable strict ARP learning.
2. Enable interface-based ARP entry restriction.
3. Enable the ARP anti-spoofing function.
4. Enable the ARP anti-attack function for preventing ARP packets with the bogus gateway address.
5. Configure the rate suppression function for ARP packets.
6. Configure the rate suppression function for ARP Miss packets.
7. Enable log and alarm functions for potential attacks.

Data Preparation

To complete the configuration, you need the following data:

- Number of limited ARP entries on the interface being 20
- Anti-spoofing mode used to prevent attacks that is initiated by User 1 being **fixed-mac**
- IP address of the server being 2.2.2.2/24
- IP address of User 4 that sends a large number of ARP packets being 2.2.4.2/24
- Maximum suppression rate for ARP packets of User 4 being 10 pps and maximum suppression rate for ARP packets of other users being 15 pps
- Maximum suppression rate for ARP Miss packets of common users being 20 pps and maximum suppression rate for ARP Miss packets on the server being 50 pps
- Interval for writing an ARP log and sending an alarm being 300 seconds

Procedure

Step 1 Enable strict ARP learning.

```
<Quidway> system-view
[Quidway] arp learning strict
```

Step 2 Configure interface-based ARP entry restriction.

The number of limited ARP entries on each interface is 20. The following lists the configuration of XGE 0/0/1, and the configurations of other interfaces are the same as the configuration of XGE 0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] arp-limit vlan 10 maximum 20
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 3 Enable the ARP anti-spoofing function.

Set the ARP anti-spoofing mode to **fixed-mac** to prevent ARP spoofing attacks initiated by User 1.

```
[Quidway] arp anti-attack entry-check fixed-mac enable
```

Step 4 Enable the ARP anti-attack function for preventing ARP packets with the bogus gateway address.

Enable the ARP anti-attack function for preventing ARP packets with the bogus gateway address to prevent User 1 from sending ARP packets with the bogus gateway address.

```
[Quidway] arp anti-attack gateway-duplicate enable
```

Step 5 Configure the rate suppression function for ARP packets.

Set the suppression rate for ARP packets sent by User 4 to 10 pps. To prevent all users from sending a large number of ARP packets incorrectly, set the suppression rate for ARP packets of the system to 15 pps.

```
[Quidway] arp speed-limit source-ip maximum 15
[Quidway] arp speed-limit source-ip 2.2.2.4 maximum 10
```

Step 6 Configure the rate suppression function for ARP Miss packets.

Set the suppression rate for ARP Miss packets of the system to 20 pps to prevent users from sending a large number of IP packets with an unreachable destination IP address.

```
[Quidway] arp-miss speed-limit source-ip maximum 20
```

Set the suppression rate for ARP Miss packets on the server to 50 pps to prevent the server from sending a large number of IP packets with an unreachable destination IP address, and to prevent communication on the network when the rate for the server to send IP packets with an unreachable destination IP address is not as required.

```
[Quidway] arp-miss speed-limit source-ip 2.2.2.2 maximum 50
```

Step 7 Enable log and alarm functions for potential attacks.

```
[Quidway] arp anti-attack log-trap-timer 300
```

Step 8 Verify the configuration.

After the configuration, run the **display arp learning strict** command, and you can view information about strict ARP learning.

```
<Quidway> display arp learning strict
 The global configuration:arp learning strict
```

```
 interface                           LearningStrictState
-------------------------------------------------------------
-------------------------------------------------------------
 Total:0
 force-enable:0
 force-disable:0
```

You can use the **display arp-limit** command to check the maximum number of ARP entries learned by the interface.

```
<Quidway> display arp-limit interface xgigabitethernet 0/0/1
 interface                     LimitNum   VlanID     LearnedNum(Mainboard)
-------------------------------------------------------------------------
 XGigabitEthernet0/0/1          20         10         0
-------------------------------------------------------------------------
 Total:1
```

You can use the **display arp anti-attack configuration all** command to check the configuration of ARP anti-attack.

```
<Quidway> display arp anti-attack configuration all
 ARP anti-attack entry-check mode: fixed-MAC

 ARP gateway-duplicate anti-attack function: enabled

 ARP anti-attack log-trap-timer: 30seconds
 (The log and trap timer of speed-limit, default is 0 and means disabled.)

ARP rate-limit configuration:
-------------------------------------------------------------------------------
 Globle configuration:
 Interface configuration:
 Vlan configuration:
-------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
-------------------------------------------------------------------------------
 Globle configuration:
 Interface configuration:
 Vlan configuration:
-------------------------------------------------------------------------------

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 2.2.4.2             10
 Others              15
 ------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 1024 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 2.2.2.2             50
 Others              20
 ------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 1024 items.
```

You can use the **display arp packet statistics** command to view the number of discarded ARP packets and the number of learned ARP entries. In addition, you can also use the **display arp anti-attack gateway-duplicate item** command to view information about attacks from the packets with the forged gateway address on the current network.

```
<Quidway> display arp packet statistics
ARP Pkt Received:   sum    167
ARP Learnt Count:   sum      8
ARP Pkt Discard For Limit:   sum      5
```

```
ARP Pkt Discard For SpeedLimit:   sum      0
ARP Pkt Discard For Other:   sum      3
<Quidway> display arp anti-attack gateway-duplicate item
 interface               IP address       MAC address     VLANID   aging time
--------------------------------------------------------------------------------
 XGigabitEthernet0/0/1    2.1.1.1          0000-0000-0002  2        153
 XGigabitEthernet0/0/2    2.1.1.2          0000-0000-0004  2        179
--------------------------------------------------------------------------------
There are 2 records in gateway conflict table
```

----End

Configuration Files

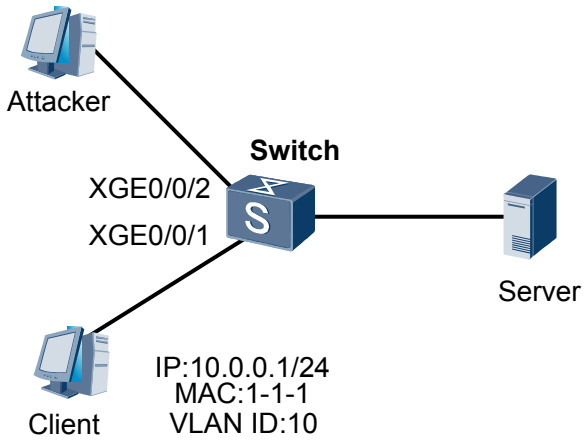
```
#
 sysname Quidway
#
vlan batch 10 20 30
#
 arp speed-limit source-ip maximum 15
 arp-miss speed-limit source-ip maximum 20
 arp learning strict
 arp anti-attack log-trap-timer 300
#
 arp anti-attack entry-check fixed-mac enable
 arp anti-attack gateway-duplicate enable
 arp-miss speed-limit source-ip 2.2.2.2 maximum 50
 arp speed-limit source-ip 2.2.4.2 maximum 10
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid tagged vlan 10
 arp-limit vlan 10 maximum 20
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid tagged vlan 20
 arp-limit vlan 20 maximum 20
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
 arp-limit vlan 30 maximum 20
#
return
```

6.4.2 Example for Configuring ARP Anti-Attack to Prevent Man-in-the-Middle Attacks

Networking Requirements

As shown in **Figure 6-13**, two users are connected to the Switch through XGE 0/0/1 and XGE 0/0/2 respectively. Assume that the user connected to XGE 0/0/2 is an attacker. To prevent the man-in-the-middle attacks, you can configure the IP source guard function. After the IP source guard function is configured on the Switch, the Switch checks the IP packets according to the binding table. Only the IP packets that match the content of the binding table can be forwarded; the other IP packets are discarded. In addition, you can enable the alarm function for discarded packets.

Figure 6-13 Networking diagram for prevent man-in-the-middle attacks



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the IP source guard function.
2. Configure the check items for ARP packets.
3. Configure a static binding table.
4. Enable the alarm function for discarded packets.

Data Preparation

To complete the configuration, you need the following data:

- Interfaces enabled with IP source guard: XGE 0/0/1 and XGE 0/0/2
- Check items: IP address + MAC address + VLAN
- Alarm threshold of the number of discarded ARP packets: 80
- IP address of the client configured in the static binding table: 10.0.0.1/2; MAC address: 1-1-1; VLAN ID: 10

Procedure

Step 1 Configure the IP source guard function.

Enable the IP source guard function on XGE 0/0/1 connected to the client.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] arp anti-attack check user-bind enable
[Quidway-XGigabitEthernet0/0/1] arp anti-attack check user-bind check-item ip-address mac-address vlan
```

Enable the IP source guard function on XGE 0/0/2 connected to the attacker.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] arp anti-attack check user-bind enable
[Quidway-XGigabitEthernet0/0/2] arp anti-attack check user-bind check-item ip-address mac-address vlan
```

Step 2 Configure the alarm function for discarded packets.

Set the alarm threshold of the ARP packets discarded because they do not match the binding table on XGE 0/0/1 connected to the client.

```
[Quidway-XGigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
[Quidway-XGigabitEthernet0/0/1] arp anti-attack check user-bind alarm threshold 80
[Quidway-XGigabitEthernet0/0/1] quit
```

Set the alarm threshold of the ARP packets discarded because they do not match the binding table on XGE 0/0/2 connected to the attacker.

```
[Quidway-XGigabitEthernet0/0/2] arp anti-attack check user-bind alarm enable
[Quidway-XGigabitEthernet0/0/2] arp anti-attack check user-bind alarm threshold 80
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 3 Configure the check items of the static binding table.

Configure Client in the static binding table.

```
[Quidway] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001
interface xgigabitethernet 0/0/1 vlan 10
```

Step 4 Verify the configuration.

Run the **display arp anti-attack configuration check user-bind interface** command, and you can view the configuration of the IP source guard function on the interface.

```
<Quidway> display arp anti-attack configuration check user-bind interface
xgigabitethernet 0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
 arp anti-attack check user-bind check-item ip-address mac-address vlan
 ARP packet drop count = 0
<Quidway> display arp anti-attack configuration check user-bind interface
xgigabitethernet 0/0/2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
 arp anti-attack check user-bind check-item ip-address mac-address vlan
 ARP packet drop count = 2442
```

The preceding information indicates that XGE 0/0/1 does not discard ARP packets, whereas XGE 0/0/2 has discarded ARP packets. It indicates that the anti-attack function takes effect.

----End

Configuration Files

```
#
vlan batch 10
#
  user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
xgigabitethernet 0/0/1 vlan 10
#
interface xgigabitethernet0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address mac-address vlan
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
#
interface xgigabitethernet0/0/2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address mac-address vlan
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
```

```
#
return
```

6.5 Source IP Attack Defense Configuration

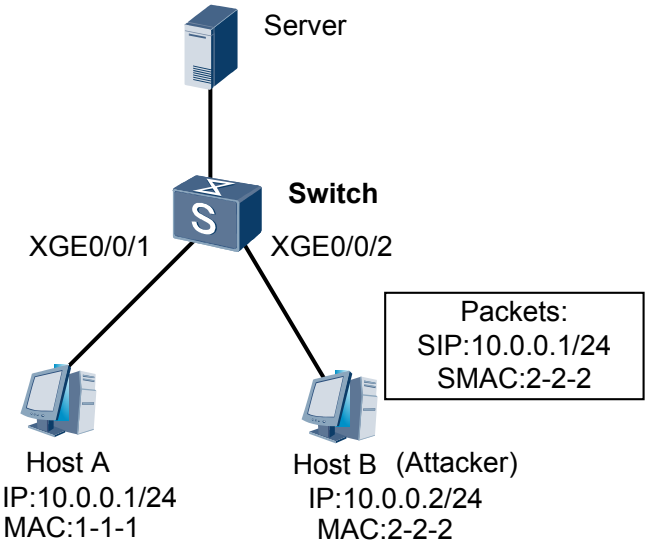
This chapter describes the principle and configuration of attacking IP source addresses.

6.5.1 Example for Configuring IP Source Guard

Networking Requirements

As shown in **Figure 6-14**, Host A is connected to the Switch through XGE 0/0/1 and Host B is connected to the Switch through XGE 0/0/2. You need to configure the IP source guard function on the Switch so that Host B cannot forge the IP address and MAC address on Host A and the IP packets from Host A can be sent to the server.

Figure 6-14 Networking diagram for configuring IP source guard



Configuration Roadmap

Assume that the user obtains an IP address through DHCP. The configuration roadmap is as follows:

1. Enable the IP source guard function on the interfaces connected to Host A and Host B.
2. Configure a static binding table.

Data Preparation

To complete the configuration, you need the following data:

- Interface connected to Host A: XGE 0/0/1; interface connected to Host B: XGE 0/0/2

- IP address of Host A: 10.0.0.1/24; MAC address of Host A: 1-1-1
- VLAN where Host A resides: VLAN 10

NOTE

This configuration example provides only the commands related to the IP Source Guard configuration.

Procedure

Step 1 Enable the IP source guard function.

Enable the IP source guard function on XGE 0/0/1 connected to Host A.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] ip source check user-bind enable
```

Enable the alarm function for checking the received IP packets on XGE 0/0/1 connected to Host A.

```
[Quidway-XGigabitEthernet0/0/1] ip source check user-bind alarm enable
[Quidway-XGigabitEthernet0/0/1] ip source check user-bind alarm threshold 200
[Quidway-XGigabitEthernet0/0/1] quit
```

Enable the IP source guard function on XGE 0/0/2 connected to Host B.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] ip source check user-bind enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Enable the alarm function for checking the received IP packets on XGE 0/0/2 connected to Host B.

```
[Quidway-XGigabitEthernet0/0/2] ip source check user-bind alarm enable
[Quidway-XGigabitEthernet0/0/2] ip source check user-bind alarm threshold 200
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 After user A goes online, the system allocates IP address 10.0.0.1/24 to the user and the user adopts MAC address 1-1-1.

Step 3 Verify the configuration.

Run the **display dhcp snooping user-bind all** command on the Switch to view information about the binding table.

```
<Quidway> display dhcp snooping user-bind all
DHCP static Bind-table:,Flags:O - outer vlan ,I - inner vlan ,P - map vlan,
IP Address                      MAC Address     VSI/VLAN(O/I/P) Interface,
-------------------------------------------------------------------------------,
 10.0.0.1                        0001-0001-0001  10  /--  /--    XGE0/0/1,
-------------------------------------------------------------------------------,
print count:           1          total count:           1,
```

The preceding information indicates that Host A exists in the static binding table, whereas Host B does not exist.

----End

Configuration Files

```
#
  user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
XGigabitEthernet 0/0/1 vlan 10
#
interface XGigabitEthernet 0/0/1
 ip source check user-bind enable
```

```
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
interface XGigabitEthernet 0/0/2
 ip source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
return
```

6.6 Local Attack Defense Configuration

This chapter describes the principle and configuration of local attack defense.

6.6.1 Example for Configuring an Attack Defense Policy

This section provides an example of configuring an attack defense policy, including the configuration of ACL, attack defense policy, the rule for sending packets to the CPU and application of the attack defense policy.

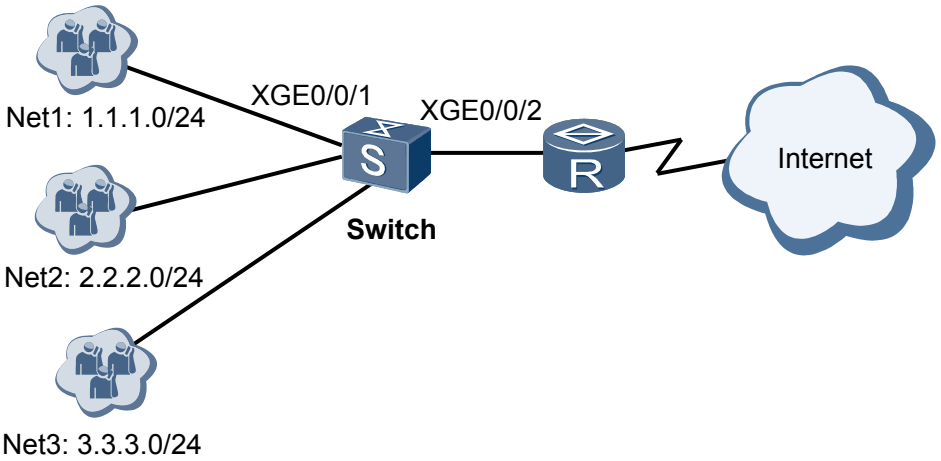
Networking Requirements

As shown in **Figure 6-15**, three local user networks net1, net2 and net3 access the Internet through the Switch. The Switch is connected to a large number of users, and receives many packets to be sent to the CPU. In this case, the CPU of the Switch may be attacked by packets directing at the CPU. To protect the CPU and enable the Switch to process services normally, you need to configure local attack defense.

You need to configure the following attack defense features on the Switch:

- Users on net1 often attack the network and are added to the blacklist. In this manner, they cannot access the network.
- Set the CAR for sending ARP Request packets to the CPU to prevent attacks of ARP Request packets.
- Set the CIR for sending FTP packets to the CPU when FTP connections are set up.

Figure 6-15 Networking diagram for configuring the attack defense policy



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the ACL and define rules for filtering the packets to be sent to the CPU.
2. Create an attack defense policy and configure the whitelist, blacklist, and user-defined flow.
3. Configure the rule for sending packets to the CPU.
4. Apply the attack defense policy.

Data Preparation

To complete the configuration, you need the following data:

- Name of the attack defense policy
- IDs of the blacklist
- ACL rule and number
- Rate of sending ARP Requests packets to the CPU
- Rate limit of sending FTP packets to the CPU when FTP connection is set up

Procedure

Step 1 Configure the rule for filtering packets to be sent to the CPU.

Define ACL rules.

```
<Quidway> system-view
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 1.1.1.0 0.0.0.255
[Quidway-acl-basic-2001] quit
```

Step 2 Create an attack defense policy.

Create an attack defense policy and configure the blacklist.

```
[Quidway] cpu-defend policy test1
[Quidway-cpu-defend-policy-test1] blacklist 1 acl 2001
```

Step 3 Configure the rule for sending packets to the CPU.

Set the CIR for ARP Request packets.

```
[Quidway-cpu-defend-policy-test1] car packet-type arp-request cir 128
```

Set the CIR for sending FTP packets to the CPU when FTP connections are set up.

```
[Quidway-cpu-defend-policy-test1] link-car packet-type ftp cir 128
[Quidway-cpu-defend-policy-test1] quit
```

Step 4 Apply the attack defense policy.

```
[Quidway] cpu-defend-policy test1 global
```

Step 5 Verify the configuration.

View information about the configured attack defense policy.

```
<Quidway> display cpu-defend policy test1
 Related slot : <0>
 Configuration :
   Blacklist 1 ACL number : 2001
   Car packet-type arp-request : CIR(128)  CBS(24064)
   Car all-packets pps : 500 (default)
```

View information about CAR.

```
<Quidway> display cpu-defend arp-request configuration all
Car Configurations On Slot 0.
------------------------------------------------------------------------------
Packet Name           Status   Cir(Kbps)   Cbs(Byte)  Queue  Port-Type
------------------------------------------------------------------------------
arp-request           Enabled    128       24064        2    UNI
------------------------------------------------------------------------------
```

----End

Configuration Files

```
#
acl number 2001
 rule 5 permit source 1.1.1.0 0.0.0.255
#
cpu-defend policy test1
 blacklist 1 acl 2001
 car packet-type arp-request cir 5000 cbs 24064
 link-car packet-type ftp cir 5000 cbs 24064
#
 cpu-defend-policy test1 global
#
return
```

6.7 PPPoE+ Configuration

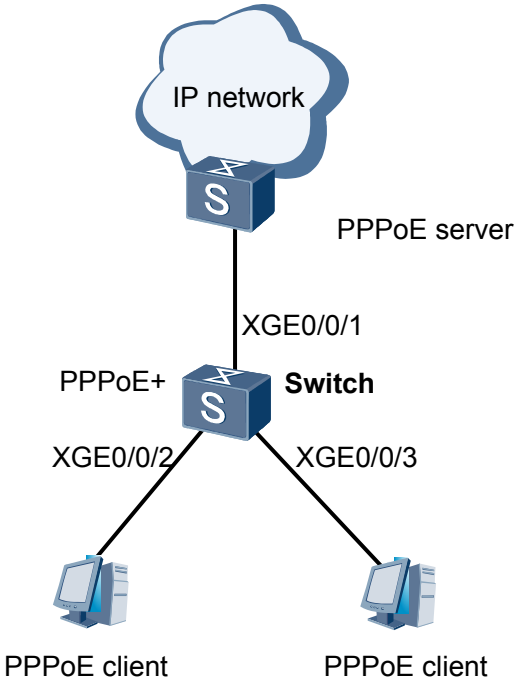
This chapter describes how to configure PPPoE+.

6.7.1 Example for Configuring PPPoE+

Networking Requirements

As shown in **Figure 6-16**, the Switch is connected to the upstream device BRAS and the downstream device PC; the PPPoE server is configured on the BRAS device. PPPoE+ is enabled on the Switch to control and monitor dialup users.

Figure 6-16 Networking diagram for configuring PPPoE+



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable PPPoE+ globally.

   NOTE

   After PPPoE+ is enabled globally, PPPoE+ is enabled on all the interfaces.
2. Configure the contents and format of fields to be added to PPPoE packets on the Switch.
3. Configure the action for the Switch to process PPPoE packets.
4. Configure the interface connecting the Switch and the PPPoE server as the trusted interface.

Data Preparation

None.

Procedure

Step 1 Enable PPPoE+.

```
<Quidway> system-view
[Quidway] pppoe intermediate-agent information enable
```

Step 2 Configure the format of information fields.

Configure the Switch to add the circuit ID in **extend** format to PPPoE packets, that is, the format in hexadecimal notation is used.

```
[Quidway] pppoe intermediate-agent information format circuit-id extend
```

Step 3 Configure the action for processing original fields in PPPoE packets.

Configure all the interfaces to replace original fields in PPPoE packets with the circuit ID of the Switch.

```
[Quidway] pppoe intermediate-agent information policy replace
```

Step 4 Configure the trusted interface.

Configure XGE 0/0/1 as the trusted interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] pppoe uplink-port trusted
[Quidway-XGigabitEthernet0/0/1] quit
```

----End

Configuration Files

```
#
 sysname Quidway
#
 pppoe intermediate-agent information enable
 pppoe intermediate-agent information format circuit-id extend
#
interface XGigabitEthernet0/0/1
 pppoe uplink-port trusted
#
return
```

6.8 MFF Configuration

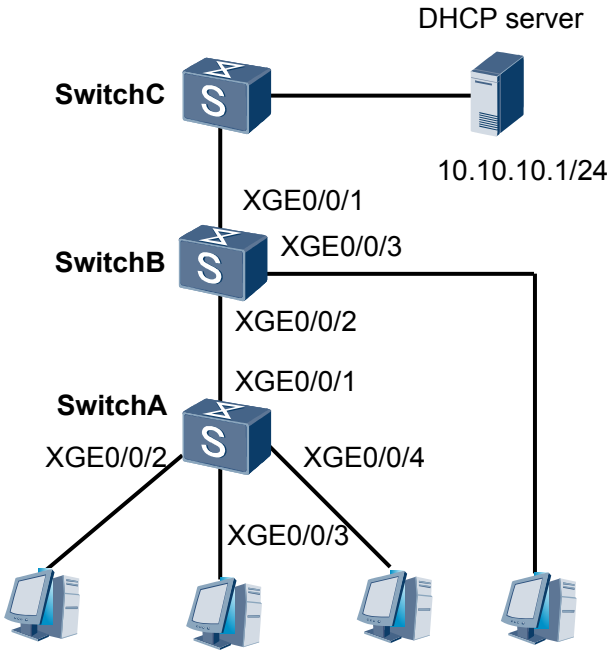
This section describes the principle and configuration of the MAC-Forced Forwarding (MFF) function.

6.8.1 Example for Configuring MFF

Networking Requirements

As shown in **Figure 6-17**, all the user hosts obtain IP addresses through the DHCP server and all the devices are located in VLAN 10. To implement Layer 2 isolation and Layer 3 interconnection between the hosts, you need to configure the MFF function on Switch A and Switch B.

Figure 6-17 Networking diagram for configuring MFF



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure DHCP snooping.
2. Enable global MFF.
3. Configure the MFF network interfaces.
4. Enable MFF for the VLAN.
5. (Optional) Enable the function of timed gateway address detection.
6. (Optional) Configure the server.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of the MFF device
- Type and number of the network interface to be configured
- (Optional) IP address of the server to be configured

Procedure

Step 1 Configure DHCP snooping.

Enable global DHCP snooping on Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable
```

Enable DHCP snooping on the interfaces of the Switch A. Take the configuration on XGE 0/0/1 as an example. The configurations on XGE 0/0/2, XGE 0/0/3, and XGE 0/0/4 are similar to the configuration on XGE 0/0/1 and are not mentioned here.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] dhcp snooping enable
[SwitchA-XGigabitEthernet0/0/1] quit
```

Set the status of interface XGE 0/0/1 on Switch A to Trusted.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] dhcp snooping trusted
[SwitchA-XGigabitEthernet0/0/1] quit
```

Enable global DHCP snooping on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] dhcp enable
[SwitchB] dhcp snooping enable
```

Enable DHCP snooping on the interfaces of the Switch B. Take the configuration on XGE 0/0/1 as an example. The configurations on XGE 0/0/2 is similar to the configuration on XGE 0/0/1 and are not mentioned here.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] dhcp snooping enable
[SwitchB-XGigabitEthernet0/0/1] quit
```

Set the status of interface XGE 0/0/1 on Switch B to Trusted.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] dhcp snooping trusted
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 2 Enable global MFF.

Enable global MFF on Switch A.

```
[SwitchA] mac-forced-forwarding enable
```

Enable global MFF on Switch B.

```
[SwitchB] mac-forced-forwarding enable
```

Step 3 Configure the MFF network interfaces.

Configure XGE 0/0/1 of Switch A as the network interface.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] mac-forced-forwarding network-port
[SwitchA-XGigabitEthernet0/0/1] quit
```

Configure XGE 0/0/2 of Switch B as the network interfaces.

```
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] mac-forced-forwarding network-port
[SwitchB-XGigabitEthernet0/0/2] quit
```

Step 4 Enable MFF for the VLAN.

Enable MFF for VLAN 10 on Switch A.

```
[SwitchA] vlan 10
[SwitchA-vlan10] mac-forced-forwarding enable
```

Enable MFF for VLAN 10 on Switch B.

```
[SwitchB] vlan 10
[SwitchB-vlan10] mac-forced-forwarding enable
```

Step 5 (Optional) Enable the function of timed gateway address detection.

Enable the function of timed gateway address detection on Switch A.

```
[SwitchA-vlan10] mac-forced-forwarding gateway-detect
```

Enable the function of timed gateway address detection on Switch B.

```
[SwitchB-vlan10] mac-forced-forwarding gateway-detect
```

Step 6 (Optional) Configure the server.

Configure the server on Switch A.

```
[SwitchA-vlan10] mac-forced-forwarding server 10.10.10.1
```

Configure the server on Switch B.

```
[SwitchB-vlan10] mac-forced-forwarding server 10.10.10.1
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan 10
#
dhcp enable
dhcp snooping enable
mac-forced-forwarding enable
#
vlan 10
 mac-forced-forwarding enable
 mac-forced-forwarding gateway-detect
 mac-forced-forwarding server 10.10.10.1
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 dhcp snooping enable
 dhcp snooping trusted
 mac-forced-forwarding network-port
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface XGigabitEthernet0/0/3
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping enable
 #
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
```

```
#
 vlan 10
#
dhcp enable
dhcp snooping enable
mac-forced-forwarding enable
#
vlan 10
 mac-forced-forwarding enable
 mac-forced-forwarding gateway-detect
 mac-forced-forwarding server 10.10.10.1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping enable
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 dhcp snooping enable
 mac-forced-forwarding network-port
#
return
```

6.9 Traffic Suppression Configuration

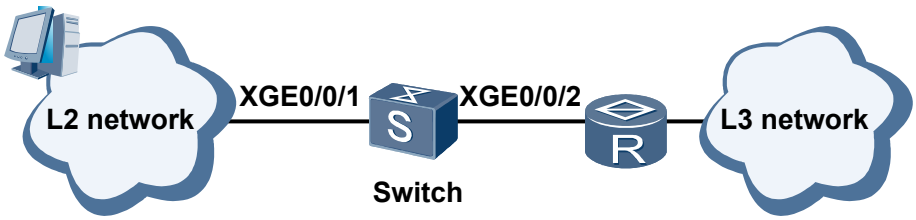
This chapter describes the principle and configuration of traffic suppression .

6.9.1 Example for Configuring Traffic Suppression

Networking Requirements

As shown in **Figure 6-18**, the Switch is connected to the Layer 2 network and Layer 3 router. To limit the number of broadcast, multicast, or unknown unicast packets forwarded on the Layer 2 network, you can configure traffic suppression on XGE 0/0/1.

Figure 6-18 Networking diagram for configuring traffic suppression



Configuration Roadmap

Configure traffic suppression in the interface view of XGE 0/0/1.

Data Preparation

To complete the configuration, you need the following data:

- XGE 0/0/1 where traffic suppression is configured
- Traffic suppression for broadcast, unknown unicast and multicast packets based on the rate percentage
- Maximum rate of broadcast, unknown unicast and multicast packets being 80 percent of the interface rate after traffic suppression is configured

Procedure

Step 1 Enter the interface view.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/1
```

Step 2 Configure traffic suppression for broadcast packets.

```
[Quidway-XGigabitEthernet0/0/1] broadcast-suppression 80
```

Step 3 Configure traffic suppression for multicast packets.

```
[Quidway-XGigabitEthernet0/0/1] multicast-suppression 80
```

Step 4 Configure traffic suppression for unknown unicast packets.

```
[Quidway-XGigabitEthernet0/0/1] unicast-suppression 80
```

Step 5 Verify the configuration.

Run the **display flow-suppression interface** command, and you can view the configuration of traffic suppression on XGE 0/0/1.

```
<Quidway> display flow-suppression interface xgigabitethernet 0/0/1
 storm type          rate mode    set rate value
-------------------------------------------------------------------------------
 unknown-unicast     percent          percent: 80%
 multicast           percent          percent: 80%
 broadcast           percent          percent: 80%
-------------------------------------------------------------------------------
```

----End

Configuration Files

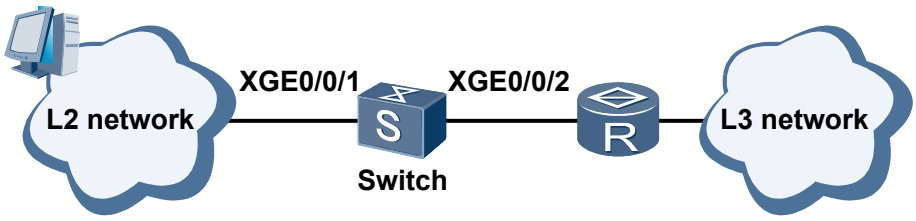
```
#
 sysname Quidway
#
interface xgigabitethernet0/0/1
 unicast-suppression 80
 multicast-suppression 80
 broadcast-suppression 80
#
return
```

6.9.2 Example for Configuring the Storm Control Function

Networking Requirements

As shown in **Figure 6-19**, when receiving unknown unicast packets, multicast packets, or broadcast packets, the Switch forwards the packets to all the interfaces except the receiving interface because the Switch cannot determine the outbound interface according to the destination MAC address of packets. In this case, broadcast storms may occur on the network. The forwarding performance of the Switch is thus reduced. The Switch is connected to the Layer 2 network and Layer 3 router. To perform storm control for broadcast packets, multicast packets, or unknown unicast packets in a VLAN, you can configure storm control on XGE 0/0/1.

Figure 6-19 Networking of storm control



Configuration Roadmap

The configuration roadmap is as follows:

- Configure storm control on XGE 0/0/1.

Data Preparation

To complete the configuration, you need the following data:

- Interface where storm control is configured being XGE 0/0/1
- Upper and lower thresholds of the rates of receiving broadcast packets, multicast packets, or unknown unicast packets
- Storm control action
- Interval for detecting storms

Procedure

Step 1 Enter the interface view.

```
<Quidway> system-view
[Quidway] interface xgigabitethernet 0/0/1
```

Step 2 Configure storm control for broadcast packets.

```
[Quidway-XGigabitEthernet0/0/1] storm-control broadcast min-rate 1000 max-rate 2000
```

Step 3 Configure storm control for multicast packets.

```
[Quidway-XGigabitEthernet0/0/1] storm-control multicast min-rate 1000 max-rate 2000
```

Step 4 Configure storm control for unknown unicast packets.

```
[Quidway-XGigabitEthernet0/0/1] storm-control unicast min-rate 1000 max-rate 2000
```

Step 5 Set the storm control action to **block**.

```
[Quidway-XGigabitEthernet0/0/1] storm-control action block
```

Step 6 Enable the function of recording logs during storm control.

```
[Quidway-XGigabitEthernet0/0/1] storm-control enable log
```

Step 7 Set the interval for detecting storms.

```
[Quidway-XGigabitEthernet0/0/1] storm-control interval 90
```

Step 8 Verify the configuration.

Run the **display storm-control interface xgigabitethernet 0/0/1** command, and you can view the storm control configuration on XGE 0/0/1.

```
<Quidway> display storm-control interface xgigabitethernet 0/0/1
PortName      Type  Rate      Action    Punish-   Trap Log Interval Last-
                    (Min/Max)           Status                      Punish-Time
-------------------------------------------------------------------------------
XGE0/0/1  Multicast  1000    Block      shutdown   off  off 90      2010-12-12
                    /2000                                        14:34:00
XGE0/0/1  Broadcast  1000    Block      shutdown   off  off 90      2010-12-12
                    /2000                                        14:30:00
XGE0/0/1  Unicast    1000    Block      shutdown   off  off 90      2010-12-12
                    /2000                                        14:36:00
```

----End

Configuration Files

```
#
interface XGigabitEthernet0/0/1
 storm-control broadcast min-rate 1000 max-rate 2000
 storm-control multicast min-rate 1000 max-rate 2000
 storm-control unicast min-rate 1000 max-rate 2000
 storm-control interval 90
 storm-control action block
 storm-control enable log
#
return
```

6.10 ACL Configuration

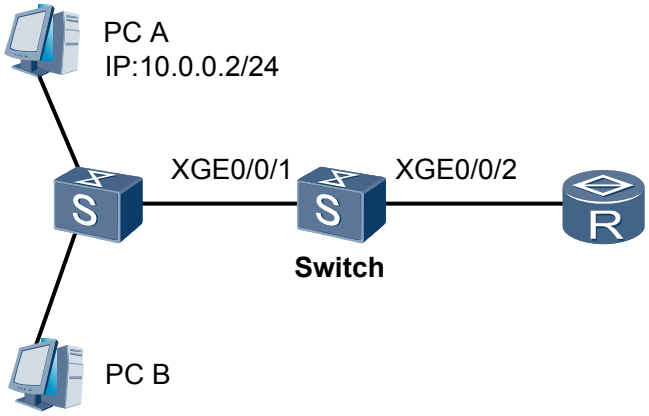
The ACL classifies packets according to the rules. After these rules are applied to the interfaces on the S6700, the S6700 can determine packets that are received and rejected.

6.10.1 Example for Configuring a Basic ACL

Networking Requirements

As shown in **Figure 6-20**, XGE 0/0/1 of the Switch is connected to the user, and XGE 0/0/2 is connected to the upstream router. It is required that the Switch does not trusts the packets from user A whose IP address is 10.0.0.2/24.

Figure 6-20 Networking diagram for configuring a basic ACL



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the ACL.
2. Configure the traffic classifier.
3. Configure the traffic behavior.
4. Configure the traffic policy.
5. Apply the traffic policy to an interface.

Data Preparation

To complete the configuration, you need the following data:

- ACL number
- IP address of user A
- Names of traffic classifier, traffic behavior, and traffic policy
- Interface where the traffic policy is applied

Procedure

Step 1 Configure the traffic classifier that is based on the ACL rules.

Define the ACL rules.

```
[Quidway] acl 2000
[Quidway-acl-basic-2000] rule permit source 10.0.0.2 0.0.0.255
[Quidway-acl-basic-2000] quit
```

Configure the traffic classifier and define the ACL rules.

```
[Quidway] traffic classifier tc1
[Quidway-classifier-tc1] if-match acl 2000
[Quidway-classifier-tc1] quit
```

Step 2 Configure the traffic behavior.

```
[Quidway] traffic behavior tb1
[Quidway-behavior-tb1] deny
[Quidway-behavior-tb1] quit
```

Step 3 Configure the traffic policy.

Define the traffic policy and associate the traffic classifier and traffic behavior with the traffic policy.

```
[Quidway] traffic policy tp1
[Quidway-trafficpolicy-tp1] classifier tc1 behavior tb1
[Quidway-trafficpolicy-tp1] quit
```

Apply the traffic policy to XGE 0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] traffic-policy tp1 inbound
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 4 Verify the configuration.

Check the configuration of the ACL rules.

```
<Quidway> display acl 2000
Basic ACL 2000, 1 rule
```

```
Acl's step is 5
 rule 5 permit source 10.0.0.0 0.0.0.255
```

Check the configuration of the traffic classifier.

```
<Quidway> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match acl 2000
```

Check the configuration of the traffic policy.

```
<Quidway>  display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
     Classifier: tc1
      Operator: AND
       Behavior: tb1
        Deny
```

----End

Configuration Files

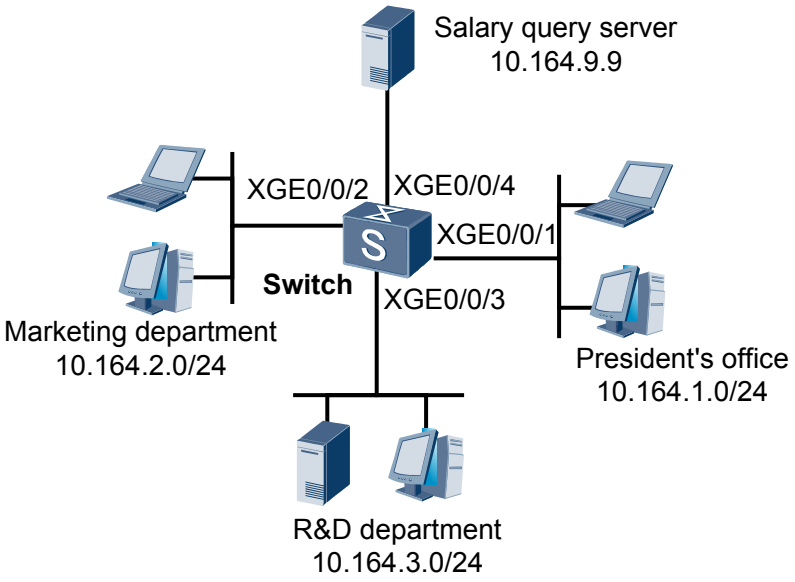
```
#
acl number 2000
 rule 5 permit source 10.0.0.0 0.0.0.255
#
traffic classifier tc1 operator and
 if-match acl 2000
#
traffic behavior tb1
  deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface XGigabitEthernet0/0/1
 traffic-policy tp1 inbound
#
return
```

6.10.2 Example for Configuring an Advanced ACL

Networking Requirements

As shown in **Figure 6-21**, the departments of the company are connected through the Switchs. It is required that the IPv4 ACL be configured correctly. The personnel of the R&D department and marketing department cannot access the salary query server at 10.164.9.9 from 8:00 to 17:30, whereas the personnel of the president's office can access the server at any time.

Figure 6-21 Networking diagram for configuring IPv4 ACLs



Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to interfaces.
2. Configure the time range.
3. Configure the ACL.
4. Configure the traffic classifier.
5. Configure the traffic behavior.
6. Configure the traffic policy.
7. Apply the traffic policy to an interface.

Data Preparation

To complete the configuration, you need the following data:

- VLAN that the interface belongs to
- Name of the time range
- ACL ID and rules
- Name of the traffic classifier and classification rules
- Name of the traffic behavior and actions
- Name of the traffic policy, and traffic classifier and traffic behavior associated with the traffic policy
- Interface that a traffic policy is applied to

Procedure

Step 1 Assign IP addresses to interfaces.

Add interfaces to the VLAN and assign IP addresses to the VLANIF interfaces.

Add XGE 0/0/1, XGE 0/0/2, and XGE 0/0/3 to VLAN 10, VLAN 20, and VLAN 30 respectively, and add XGE 0/0/4 to VLAN 100. The first IP address of the network segment is taken as the address of the VLANIF interface. Take XGE 0/0/1 as an example. The configurations of other interfaces are similar to the configuration of XGE 0/0/1, and are not mentioned here.

```
<Quidway> system-view
[Quidway] vlan batch 10 20 30 100
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type access
[Quidway-XGigabitEthernet0/0/1] port default vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Quidway-Vlanif10] quit
```

Step 2 Configure the time range.

Configure the time range from 8:00 to 17:30.

```
<Quidway> system-view
[Quidway] time-range satime 8:00 to 17:30 working-day
```

Step 3 Configure ACLs.

Configure the ACL for the personnel of the marketing department to access the salary query server.

```
[Quidway] acl 3002
[Quidway-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination
10.164.9.9 0.0.0.0 time-range satime
[Quidway-acl-adv-3002] quit
```

Configure the ACL for the personnel of the R&D department to access the salary query server.

```
[Quidway] acl 3003
[Quidway-acl-adv-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination
10.164.9.9 0.0.0.0 time-range satime
[Quidway-acl-adv-3003] quit
```

Step 4 Configure ACL-based traffic classifiers.

Configure the traffic classifier **c_market** to classify the packets that match ACL 3002.

```
[Quidway] traffic classifier c_market
[Quidway-classifier-c_market] if-match acl 3002
[Quidway-classifier-c_market] quit
```

Configure the traffic classifier **c_rd** to classify the packets that match ACL 3003.

```
[Quidway] traffic classifier c_rd
[Quidway-classifier-c_rd] if-match acl 3003
[Quidway-classifier-c_rd] quit
```

Step 5 Configure traffic behaviors.

Configure the traffic behavior **b_market** to reject packets.

```
[Quidway] traffic behavior b_market
[Quidway-behavior-b_market] deny
[Quidway-behavior-b_market] quit
```

Configure the traffic behavior **b_rd** to reject packets.

```
[Quidway] traffic behavior b_rd
[Quidway-behavior-b_rd] deny
[Quidway-behavior-b_rd] quit
```

Step 6 Configure traffic policies.

Configure the traffic policy **p_market** and associate the traffic classifier **c_market** and the traffic behavior **b_market** with the traffic policy.

```
[Quidway] traffic policy p_market
[Quidway-trafficpolicy-p_market] classifier c_market behavior b_market
[Quidway-trafficpolicy-p_market] quit
```

Configure the traffic policy **p_rd** and associate the traffic classifier **c_rd** and the traffic behavior **b_rd** with the traffic policy.

```
[Quidway] traffic policy p_rd
[Quidway-trafficpolicy-p_rd] classifier c_rd behavior b_rd
[Quidway-trafficpolicy-p_rd] quit
```

Step 7 Apply the traffic policy.

Apply the traffic policy **p_market** to XGE 0/0/2.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] traffic-policy p_market inbound
[Quidway-XGigabitEthernet0/0/2] quit
```

Apply the traffic policy **p_rd** to XGE 0/0/3.

```
[Quidway] interface xgigabitethernet 0/0/3
[Quidway-XGigabitEthernet0/0/3] traffic-policy p_rd inbound
[Quidway-XGigabitEthernet0/0/3] quit
```

Step 8 Verify the configuration.

Check the configuration of ACL rules.

```
<Quidway> display acl all
 Total nonempty ACL number is 2

Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime (Inactive)

Advanced ACL 3003, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime (Inactive)
```

Check the configuration of the traffic classifier.

```
<Quidway> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c_market
    Operator: AND
    Rule(s) : if-match acl 3002

   Classifier: c_rd
    Operator: AND
    Rule(s) : if-match acl 3003
```

Check the configuration of the traffic policy.

```
<Quidway>  display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p_market
    Classifier: c_market
```

```
    Operator: AND
     Behavior: b_market
      Deny

  Policy: p_rd
   Classifier: c_rd
    Operator: AND
     Behavior: b_rd
      Deny
```

----End

Configuration Files

```
#
 sysname Quidway
#
 vlan batch 10 20 30 40 100
#
 time-range satime 08:00 to 17:30 working-day
#
acl number 3002
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
#
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
#
traffic classifier c_market operator or
 if-match acl 3002
traffic classifier c_rd operator or
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
#
traffic policy p_market
 classifier c_market behavior b_market
traffic policy p_rd
 classifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.1 255.255.255.0
#
interface XGE0/0/1
 port link-type access
 port default vlan 10
#
interface XGE0/0/2
 port link-type access
 port default vlan 20
 traffic-policy p_market inbound
#
interface XGE0/0/3
 port link-type access
 port default vlan 30
```

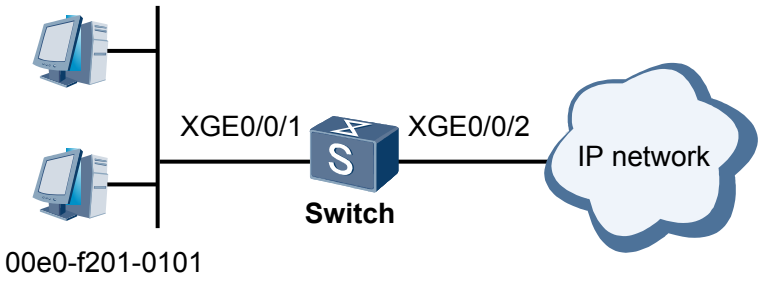
```
 traffic-policy p_rd inbound
#
interface XGE0/0/4
 port link-type access
 port default vlan 100
#
return
```

6.10.3 Example for Configuring a Layer 2 ACL

Networking Requirements

As shown in **Figure 6-22**, the Switch that functions as the gateway is connected to the PC. It is required that the ACL configured to prevent the packets with the source MAC address as 00e0-f201-0101 and the destination MAC address as 0260-e207-0002 from passing through.

Figure 6-22 Networking diagram for configuring layer 2 ACLs



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the ACL.
2. Configure the traffic classifier.
3. Configure the traffic behavior.
4. Configure the traffic policy.
5. Apply the traffic policy to an interface.

Data Preparation

To complete the configuration, you need the following data:

- ACL ID and rules
- Name of the traffic classifier and classification rules
- Name of the traffic behavior and actions
- Name of the traffic policy, and traffic classifier and traffic behavior associated with the traffic policy
- Interface that a traffic policy is applied to

Procedure

Step 1 Configure an ACL.

Configure the required layer 2 ACL.

```
[Quidway] acl 4000
[Quidway-acl-L2-4000] rule deny source-mac 00e0-f201-0101 ffff-ffff-ffff
destination-mac 0260-e207-0002 ffff-ffff-ffff
[Quidway-acl-L2-4000] quit
```

Step 2 Configure the traffic classifier that is based on the ACL.

Configure the traffic classifier **tc1** to classify packets that match ACL 4000.

```
[Quidway] traffic classifier tc1
[Quidway-classifier-tc1] if-match acl 4000
[Quidway-classifier-tc1] quit
```

Step 3 Configure the traffic behavior.

Configure the traffic behavior **tb1** to reject packets.

```
[Quidway] traffic behavior tb1
[Quidway-behavior-tb1] deny
[Quidway-behavior-tb1] quit
```

Step 4 Configure the traffic policy.

Configure the traffic policy **tp1** and associate **tc1** and **tb1** with the traffic policy.

```
[Quidway] traffic policy tp1
[Quidway-trafficpolicy-tp1] classifier tc1 behavior tb1
[Quidway-trafficpolicy-tp1] quit
```

Step 5 Apply the traffic policy.

Apply the traffic policy **tp1** to XGE 0/0/1.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] traffic-policy tp1 inbound
[Quidway-XGigabitEthernet0/0/1] quit
```

Step 6 Verify the configuration.

Check the configuration of ACL rules.

```
<Quidway> display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 deny destination-mac 0260-e207-0002 source-mac 00e0-f201-0101
```

Check the configuration of the traffic classifier.

```
<Quidway> display traffic classifier user-defined
   User Defined Classifier Information:
   Classifier: tc1
    Operator: AND
    Rule(s) : if-match acl 4000
```

Check the configuration of the traffic policy.

```
<Quidway>  display traffic policy user-defined tp1
 User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: AND
```

```
    Behavior: tb1
     Deny
```

----End

Configuration Files

```
#
 sysname Quidway
#
acl number 4000
 rule 5 deny destination-mac 0260-e207-0002 source-mac 00e0-f201-0101
#
traffic classifier tc1 operator and
 if-match acl 4000
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface XGigabitEthernet0/0/1
  traffic-policy tp1 inbound
#
return
```

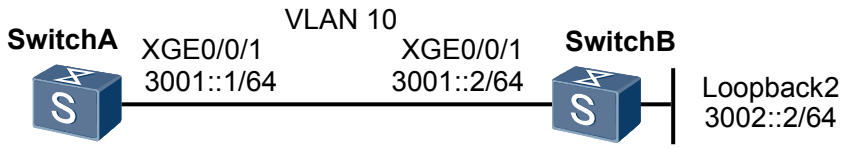
6.10.4 Example for Configuring an ACL6 to Control FTP User Access

Networking Requirements

As shown in **Figure 6-23**, the IP address of the switch that functions as the FTP server is 3002::1/64.

The routes between PC1, PC2, and the FTP server are reachable. It is required that an ACL6 be configured on the FTP server to prohibit PC2 with IP address 3001::2/64 from downloading and uploading files through FTP.

Figure 6-23 Networking diagram for configuring an ACL6 to control FTP users



Configuration Roadmap

The configuration roadmap is as follows:

1. Perform basic configurations on the FTP server.
2. Configure a basic ACL6.
3. Bind the basic ACL6 to the FTP server.

Data Preparation

To complete the configuration, you need the following data:

- FTP user name and password configured on the FTP server
- Basic ACL6 number

Procedure

Step 1 Configure basic FTP functions.

See Example for Configuring the FTP Server.

Step 2 Configure a basic ACL6.

```
<Quidway> system-view
[Quidway] acl ipv6 number 2001
[Quidway-acl-basic-2001] rule deny source 3001::2/128
[Quidway-acl-basic-2001] quit
```

Step 3 Bind the basic ACL6 to the FTP server.

```
[Quidway] ftp ipv6 acl 2001
```

Step 4 Verify the configuration.

Connect PC1 to the FTP server.

```
c:\ ftp 3002::1
Connected to 3002::1
220 FTP service ready.
User (3003::5:(none)):u1
331 Password required for u1
Password:
230 User logged in.
ftp>
```

Connect PC2 to the FTP server.

```
c:\ ftp 3002::1
Connected to 3002::1
Info:ACL6 was denied by remote host!
Connection closed by remote host.
```

----End

Configuration Files

```
#
acl ipv6 number 2001
 rule 0 deny source 3001::2/128
#
ftp ipv6 acl 2001
#
return
```

6.11 ND Snooping Configuration

This chapter describes the principle and configuration method of neighbor discovery (ND) snooping and provides configuration examples.

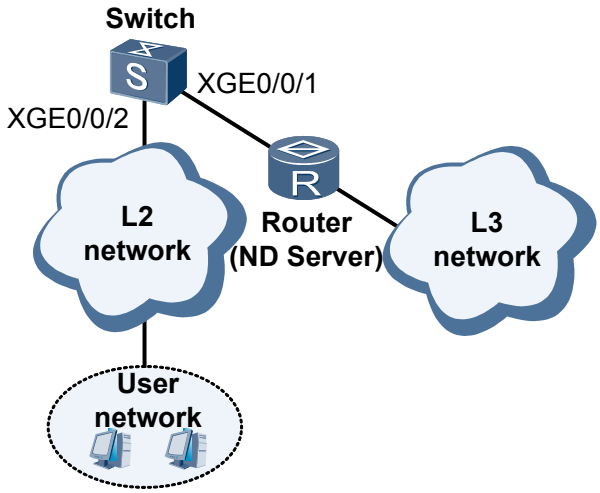
6.11.1 Example for Configuring ND Snooping on a Layer 2 Network

This section describes the procedure for configuring ND snooping, including the configuration of the trusted interface and the ND dynamic binding table.

Networking Requirements

As shown in **Figure 6-24**, the Switch is deployed in the layer 2 network between the user network and the ND server. To protect the Switch against the attacks of a bogus ND server, it is required that ND snooping be configured on the Switch and the network-side interface of the carrier be configured as the trusted interface. By maintaining the prefix management table and ND dynamic binding table, the Switch ensures that authorized users access the network and prevents unauthorized users from attacking network devices and authorized users.

Figure 6-24 Networking diagram for configuring ND snooping on a Layer 2 network



Configuration Roadmap

The configuration roadmap is as follows (assume that the ND server is configured):

1. Enable ND snooping in the system view and interface view.
2. Configure the interface connected to the ND server as the trusted interface.
3. Configure the aging function of the ND dynamic binding table.

Data Preparation

To complete the configuration, you need the following data:

- Interfaces in trusted or untrusted mode: XGE 0/0/1 in trusted mode and XGE 0/0/2 in untrusted mode
- Detection interval for aging ND dynamic binding entries
- Number of detection times for aging ND dynamic binding entries

Procedure

Step 1 Configure ND snooping.

Enable ND snooping globally.

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] nd snooping enable
```

Enable DHCP snooping an interfaces.

```
[Quidway] interface xgigabitethernet 0/0/2
[Quidway-XGigabitEthernet0/0/2] nd snooping enable
[Quidway-XGigabitEthernet0/0/2] quit
```

Step 2 Configure XGE 0/0/1 as the trusted interface.

```
[Quidway] interface xgigabitethernet 0/0/1
[Quidway-XGigabitEthernet0/0/1] nd snooping trusted
[Quidway-XGigabitEthernet0/0/1] quit
```

After ND snooping is enabled on XGE 0/0/2, the interface is the untrusted interface by default.

Step 3 Configure the aging function of the ND dynamic binding table.

Set the detection interval and the number of detection times for aging ND dynamic binding entries.

```
[Quidway] nd user-bind detect enable
[Quidway] nd user-bind detect retransmit 5 interval 600
```

Step 4 Verify the configuration.

Run the **display this** command in the system view, and you can view that ND snooping is enabled globally and on the interface.

```
[Quidway] display this
 nd snooping enable
 nd user-bind detect enable
 nd user-bind detect retransmit 5 interval 600
```

Run the **display nd snooping prefix** command, and you can view the prefix management table of ND users.

```
<Quidway> display nd snooping prefix
prefix-table:
Prefix                          Length   Valid-Time  Preferred-Time
-------------------------------------------------------------------------------
2001::                          64       600         600
Info: Prefix table total count:1
```

Run the **display nd snooping user-bind all** command, and you can view information about the ND dynamic binding table.

```
<Quidway> display nd snooping user-bind all
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                  MAC Address     VSI/VLAN(O/I/P) Lease
-------------------------------------------------------------------------------
3001::E58C:A2E7:AA4C:8E59   00e0-4c7c-af8f  30  /--  /--    2011.05.06-20:09
3001::E58C:A2E7:AA4C:8D54   00e0-4c7c-afae  30  /--  /--    2011.05.06-20:09
-------------------------------------------------------------------------------
Dynamic binditem count:        2         Dynamic binditem total count:  2
```

----End

Configuration Files

```
#
 dhcp enable
#
 nd snooping enable
#
 nd user-bind detect enable
#
 nd user-bind detect retransmit 5 interval 600
#
interface XGigabitEthernet0/0/1
 nd snooping enable
 nd snooping trusted
#
interface XGigabitEthernet0/0/2
 nd snooping enable
#
return
```

7 Configuration Guide - Reliability

About This Chapter

This document describes the configuration of DLDP, Smart Link, RRPP, EFM, BFD, VRRP and VRRP6, and MAC swap loopback to ensure reliability of Ethernet services on the S6700.

The document provides the configuration procedures and configuration examples to illustrate the service configuration methods and application scenario.

7.1 DLDP Configuration

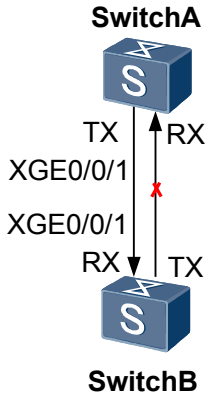
This chapter describes the principle, configuration procedure, and configuration example of the Device Link Detection Protocol (DLDP).

7.1.1 Example for Configuring DLDP

Networking Requirements

As shown in **Figure 7-1**, two S6700s are connected through a pair of optical fibers. On a fiber, RX indicate the receive end, and TX indicates the transmit end. DLDP is enabled on the interconnected interfaces. If the Rx fiber on Switch A fails, Switch A cannot receive optical signals. In this case, XGE 0/0/1 of Switch A becomes Down and cannot send or receive any packets. However, the Tx fiber on Switch B still sends optical signals, and Switch B can receive optical signals because the Tx fiber on Switch A is working normally. Therefore, the link status on Switch B is still Up. If Switch B does not receive any DLDP packet from Switch A within the neighbor aging time, XGE 0/0/1 of Switch B changes to unidirectional state. To prevent network faults, DLDP disables XGE 0/0/1 of Switch B.

Figure 7-1 Disconnection of one fiber



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the interfaces at both ends to work in non-auto-negotiation mode.
2. Enable DLDP.
3. Set the operation mode of DLDP.
4. Set the interval for sending Advertisement packets.
5. Set the Delay Down timer.
6. Set the mode of disabling the interface when a unidirectional link is detected.
7. Set the authentication mode of DLDP packets.

Data Preparation

To complete the configuration, you need the following data:

- Type and number of each interface
- Interval for sending Advertisement packets
- Value of the Delay Down timer

Procedure

Step 1 Configure the interface on Switch A to work in non-auto negotiation mode.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] undo negotiation auto
[SwitchA-XGigabitEthernet0/0/1] quit
```

Step 2 Enable DLDP globally

```
[SwitchA] dldp enable
```

Step 3 Enable DLDP on the interface.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] dldp enable
[SwitchA-XGigabitEthernet0/0/1] quit
```

Step 4 Configure DLDP to work in enhanced mode.

```
[SwitchA] dldp work-mode enhance
```

Step 5 Set the interval for sending Advertisement packets to 80 seconds.

```
[SwitchA] dldp interval 80
```

Step 6 Set the timeout interval of the DelayDown timer to 4 seconds.

```
[SwitchA] dldp delaydown-timer 4
```

Step 7 Configure DLDP to automatically shut down the interface where a unidirectional link is detected.

```
[SwitchA] dldp unidirectional-shutdown auto
```

Step 8 Set the authentication mode of DLDP packets to simple password authentication and set the password to 123456.

```
[SwitchA] dldp authentication-mode simple 12345
```

Repeat the preceding steps on Switch B.

Step 9 Verify the configuration.

After the configuration, run the **display dldp** command in the interface view, and you can find that the DLDP status of the interface is **advertisement**.

```
[SwitchA] display dldp interface xgigabitethernet 0/0/1

Interface XGigabitEthernet0/0/1
 DLDP port state: advertisement
 DLDP link state: up
 The neighbor number of the port is: 1.
   Neighbor mac address:0018-2000-0083
   Neighbor port index:27
   Neighbor state:two way
   Neighbor aged time:185
```

Remove the Rx fiber from Switch A to simulate a unidirectional link between XGE 0/0/1 of Switch A and XGE 0/0/1 of Switch B, as shown in **Figure 7-1**. You find that DLDP blocks the XGE 0/0/1 interface of Switch B.

Run the **display dldp** on Switch A, and you can find that the DLDP status of XGE 0/0/1 is inactive. Run the **display dldp** on Switch B, and you can find that the DLDP status of XGE 0/0/1 is disable.

```
[SwitchA] display dldp interface xgigabitethernet 0/0/1

Interface XGigabitEthernet0/0/1
 DLDP port state: inactive
 DLDP link state: down
 The neighbor number of the port is: 0
[SwitchB] display dldp interface xgigabitethernet 0/0/1

Interface XGigabitEthernet0/0/1
 DLDP port state: disable
 DLDP link state: up
 The neighbor number of the port is: 0
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 dldp enable
 dldp interval 80
 dldp delaydown-timer 4
 dldp authentication-mode simple 12345
#
interface XGigabitEthernet0/0/1
 dldp enable
 undo negotiation auto
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 dldp enable
 dldp interval 80
 dldp delaydown-timer 4
 dldp authentication-mode simple 12345
#
interface XGigabitEthernet0/0/1
 dldp enable
 undo negotiation auto
#
return
```

7.2 Smart Link and Monitor Link Configuration

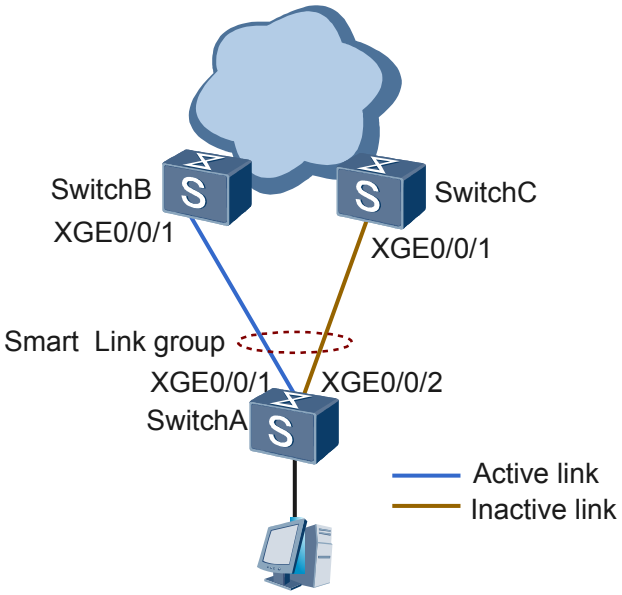
This chapter describes the principle, configuration procedure, and configuration example of the Smart Link and Monitor Link.

7.2.1 Example for Configuring Basic Functions of Smart Link

Networking Requirements

As shown in **Figure 7-2**, the user-side network is connected to the metropolitan area network (MAN) in dual-homing mode to guarantee the reliability of the network. In addition, ensure rapid switching of traffic over the standby link when the active link fails so that the duration of service interruption is limited to several milliseconds.

Figure 7-2 Networking for configuring basic functions of Smart Link



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Smart Link group on Switch A and add the uplink interfaces to the Smart Link group.
2. Enable revertive switching on Switch A.
3. Enable Switch A to send Flush packets.
4. Enable Switch B and Switch C to receive Flush packets.
5. Enable the Smart Link group on Switch A.

Data Preparation

To complete the configuration, you need the following data:

- Smart Link group ID
- Number of the uplink interface of Switch A
- Control VLAN ID and password contained in Flush packets

Procedure

Step 1 On Switch A, configure the control VLAN and add interfaces to the control VLAN.

```
<SwitchA> system-view
[SwitchA] vlan batch 10
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[SwitchA-XGigabitEthernet0/0/2] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Step 2 Add the STP-disabled uplink interface to the Smart Link group and specify it as the master or slave interface.

Configure SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] stp disable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp disable
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] port xgigabitethernet 0/0/1 master
[SwitchA-smlk-group1] port xgigabitethernet 0/0/2 slave
```

Step 3 Enable revertive switching and set the WTR time.

Configure Switch A.

```
[SwitchA-smlk-group1] restore enable
[SwitchA-smlk-group1] timer wtr 30
```

Step 4 Enable the function of sending Flush packets.

Configure Switch A.

```
[SwitchA-smlk-group1] flush send control-vlan 10 password simple 123
```

Step 5 Enable the Smart Link group on Switch A.

```
[SwitchA-smlk-group1] smart-link enable
[SwitchA-smlk-group1] quit
```

Step 6 Enable the function of receiving Flush packets.

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password
simple 123
[SwitchB-XGigabitEthernet0/0/1] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password
simple 123
[SwitchC-XGigabitEthernet0/0/1] quit
```

Step 7 Verify the configuration.

Run the **display smart-link group** command to view information about the Smart Link group on Switch A. If the following information is displayed, the configuration is successful.

- The Smart Link group is enabled.
- The control VLAN ID is 10.
- XGE 0/0/1 is the master interface and is in **Active** state, and XGE 0/0/2 is the slave interface and is in **Inactive** state.

```
[SwitchA] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1   Master Active   1           0000/00/00 00:00:00 UTC+00
:00
  XGigabitEthernet0/0/2  Slave  Inactive 0           0000/00/00 00:00:00 UTC+00
:00
```

Run the **shutdown** command to shut down XGEt 0/0/1, and you can find that XGE 0/0/1 is in **Inactive** state and XGE 0/0/2 is in **Active** state.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] undo shutdown
[SwitchA-XGigabitEthernet0/0/1]display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494  Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1   Master Inactive 1           0000/00/00 00:00:00 UTC+00
:00
  XGigabitEthernet0/0/2   Slave  Active   1           0000/00/00 00:00:00 UTC+00
:00
```

Run the **undo shutdown** command to shut down XGE 0/0/1, and you can find that XGE 0/0/1 is in **Active** state and XGE 0/0/2 is in **Inactive** state.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] undo shutdown
[SwitchA-XGigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1   Master Active   2           0000/00/00 00:00:00 UTC+00
:00
  XGigabitEthernet0/0/2   Slave  Inactive 1           0000/00/00 00:00:00 UTC+00
:00
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname Switch A
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
smart-link group 1
 restore enable
 smart-link enable
 port XGigabitEthernet0/0/1 master
 port XGigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

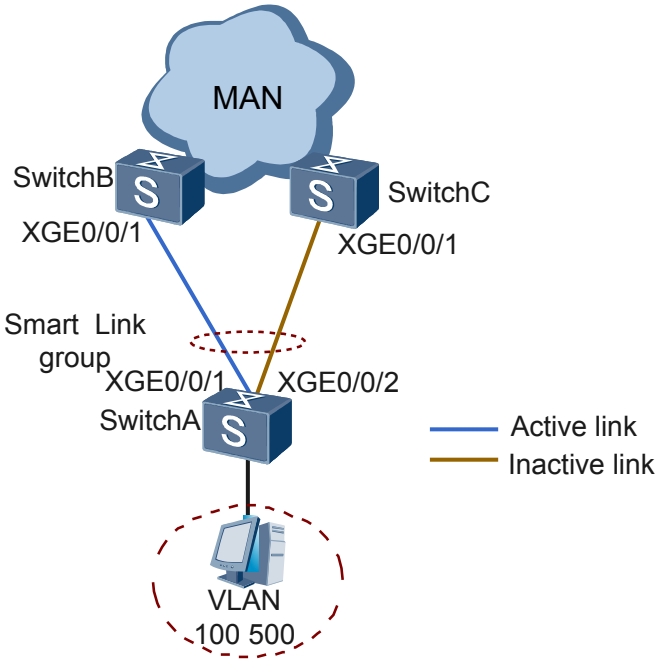
7.2.2 Example for Configuring Load Balancing Between Active and Standby Links of a Smart Link Group

Networking Requirements

As shown in **Figure 7-3**, packets of VLAN 100 and VLAN 500 are transmitted through the standby link, and packets of other VLANs are transmitted through the active link. To ensure network reliability, the customer network is dual-homed to the MAN. Packets of VLAN 100 and VLAN 500 are transmitted through the standby link, and packets of other VLANs are transmitted through the active link. When the active link fails, packets on the active link can be

switched to the standby link quickly. When the standby link fails, packets of VLAN 100 and VLAN 500 can be switched to the active link quickly. The service interruption duration is restricted to millisecond level.

Figure 7-3 Networking diagram for configuring load balancing between active and standby links of a Smart Link group



Configuration Roadmap

The configuration roadmap is as follows:

1. On Switch A, configure Smart Link multi-instance and add the uplink interfaces to the Smart Link group.
2. Configure load balancing on Switch A.
3. Enable revertive switching on Switch A.
4. Enable Switch A to send Flush packets.
5. Enable Switch B and Switch C to receive Flush packets.
6. Enable Smart Link on Switch A.

Data Preparation

To complete the configuration, you need the following data:

- IDs of instances and IDs of the VLANs bound to the instances on Switch A
- ID of a Smart Link group
- Numbers of the uplink interfaces on Switch A
- Control VLAN ID and password contained in Flush packets

Procedure

Step 1 On Switch A, configure the control VLAN and add the uplink interfaces to the control VLAN.

```
<SwitchA> system-view
[SwitchA] vlan batch 10 100 500
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10 100 500
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10 100 500
[SwitchA-XGigabitEthernet0/0/2] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Step 2 Configure VLAN mapping on Switch A.

```
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 10 vlan 100 500
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

Step 3 Add the uplink interfaces to the Smart Link group and specify the master and slave interfaces. Ensure that STP is disabled on the uplink interfaces.

Configure Switch A.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] stp disable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp disable
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] port xgigabitethernet 0/0/1 master
[SwitchA-smlk-group1] port xgigabitethernet 0/0/2 slave
```

Step 4 Configure load balancing on Switch A.

```
[SwitchA-smlk-group1] load-balance instance 10 slave
```

Step 5 Enable the revertive switching and set the wait-to-restore (WTR) time.

Configure Switch A.

```
[SwitchA-smlk-group1] restore enable
[SwitchA-smlk-group1] timer wtr 30
```

Step 6 Enable the sending of Flush packets.

Configure Switch A.

```
[SwitchA-smlk-group1] flush send control-vlan 10 password simple 123
```

Step 7 Enable Smart Link on Switch A.

```
[SwitchA-smlk-group1] smart-link enable
[SwitchA-smlk-group1] quit
```

Step 8 Enable the receiving of Flush packets.

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password
simple 123
[SwitchB-XGigabitEthernet0/0/1] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] smart-link flush receive control-vlan 10 password
simple 123
[SwitchC-XGigabitEthernet0/0/1] quit
```

Step 9 Verify the configuration.

Run the **display smart-link group** command to view information about the Smart Link group on Switch A. If the following information is displayed, it indicates that the configuration is successful.

- The Smart Link function is enabled.
- The control VLAN ID is 10.
- XGE 0/0/1 is the master interface and is in Active state, and XGE 0/0/2 is the slave interface and is in Inactive state. The load balancing function is configured.

```
[SwitchA] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 10
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
     Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1   Master Active   1           0000/00/00 00:00:00 UTC+00
:00
  XGigabitEthernet0/0/2   Slave  Inactive 0           0000/00/00 00:00:00 UTC+00
:00
```

Run the **shutdown** command to shut down XGE 0/0/1, and you can find that XGE 0/0/1 is in Inactive state and XGE 0/0/2 is in Active state.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] shutdown
[SwitchA-XGigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 10
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1   Master Inactive 1           0000/00/00 00:00:00 UTC+00
:00
  XGigabitEthernet0/0/2   Slave  Active   1           0000/00/00 00:00:00 UTC+00
:00
```

Run the **undo shutdown** command to enable XGE 0/0/1 and wait for 30 seconds. Then you can find that XGE 0/0/1 is in Active state and XGE 0/0/2 is in Inactive state.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] shutdown
[SwitchA-XGigabitEthernet0/0/1] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  Load-Balance Instance: 10
  There is no protected-vlan reference-instance
```

```
  DeviceID: 0025-9e80-2494 Control-vlan ID:
10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1   Master Active   2           0000/00/00 00:00:00 UTC+00
:00
  XGigabitEthernet0/0/2   Slave  Inactive 1           0000/00/00 00:00:00 UTC+00
:00
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10 100 500
#
stp region-configuration
 instance 10 vlan 10 100 500
 active region-configuration
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 stp disable
#
smart-link group 1
 load-balance instance 10 slave
 restore enable
 smart-link enable
 port XGigabitEthernet0/0/1 master
 port XGigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10 100 500
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 smart-link flush receive control-vlan 10 password simple 123
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 10 100 500
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100 500
 smart-link flush receive control-vlan 10 password simple 123
```

```
#
return
```

7.2.3 Example for Applying the Smart Link Functions

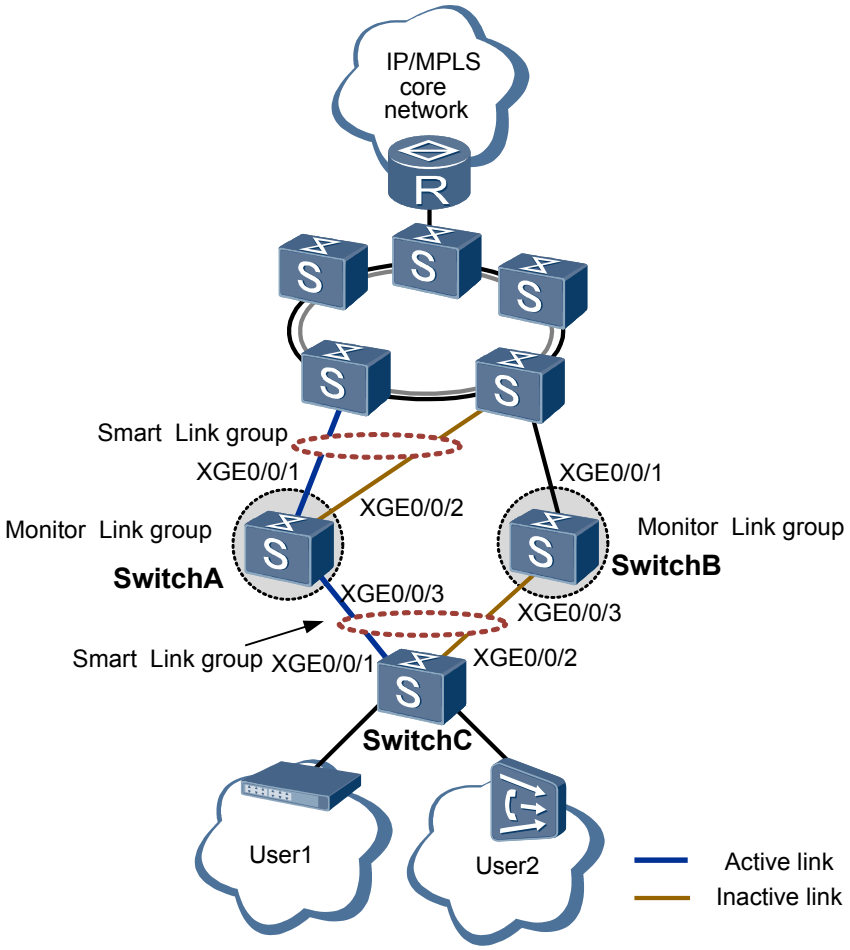
Networking Requirements

As shown in **Figure 7-4**, Switch C on the MAN is connected to user networks. It accesses the backbone network through uplink devices Switch A and Switch B in dual-homed mode.

Switch A and Switch C are connected to uplink devices in dual-homed mode. One out of each link pair needs to be blocked to prevent loops. When the active link fails, the data flows can be rapidly switched to the standby link to ensure normal services.

In addition, a monitoring mechanism is required to prevent service interruption caused by faults of the uplink. This monitoring mechanism enables the downlink to quickly detect the fault of the uplink. When the uplink fails, link switching can be performed immediately to shorten the duration of service interruption.

Figure 7-4 Networking of Smart Link application



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Smart Link groups on Switch A and Switch C, and add uplink interfaces to the groups.
2. Configure Monitor Link groups on Switch A and Switch B.
3. Enable Switch A and Switch C to send Flush packets.
4. Enable Switch A and Switch C to receive Flush packets.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of interfaces on Switch A, Switch B, and Switch C
- IDs of the Smart Link groups
- Control VLAN ID and password contained in Flush packets
- IDs of the Monitor Link groups and the numbers of the downlinks

Procedure

Step 1 Configure the same control VLAN on Switch A, Switch B, and Switch C. Add the interfaces of the Smart Link group or Monitor Link group to this VLAN.

The configuration procedures are not mentioned here. For details, see "VLAN Configuration" in the *Quidway S6700 Series Ethernet Switches Configuration Guide - Ethernet*.

Step 2 Create Smart Link groups and enable the functions of the groups.

Configure Switch A.

```
<SwitchA> system-view
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] smart-link group 2
[SwitchC-smlk-group2] quit
```

Step 3 Add interfaces to Smart Link groups and specify the master and slave interfaces of each Smart Link group

Configure Switch A.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] stp disable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp disable
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA]smart-link group 1
[SwitchA-smlk-group1] port xgigabitethernet 0/0/1 master
[SwitchA-smlk-group1] port xgigabitethernet 0/0/2 slave
```

Configure Switch C.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] stp disable
```

```
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] stp disable
[SwitchC-XGigabitEthernet0/0/2] quit
[SwitchC] smart-link group 2
[SwitchC-smlk-group2] port xgigabitethernet 0/0/1 master
[SwitchC-smlk-group2] port xgigabitethernet 0/0/2 slave
```

Step 4 Enable revertive switching and set the interval of revertive switching.

Configure Switch A.

```
[SwitchA-smlk-group1] restore enable
[SwitchA-smlk-group1] timer wtr 30
```

Configure Switch C.

```
[SwitchC-smlk-group2] restore enable
[SwitchC-smlk-group2] timer wtr 30
```

Step 5 Enable the sending and receiving of Flush packets.

Configure Switch A.

```
[SwitchA-smlk-group1] flush send control-vlan 10 password simple 123
[SwitchA-smlk-group1] quit
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] smart-link flush receive control-vlan 10 password
simple 123
[SwitchA-XGigabitEthernet0/0/3] quit
```

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] interface xgigabitethernet 0/0/3
[SwitchB-XGigabitEthernet0/0/3] smart-link flush receive control-vlan 10 password
simple 123
[SwitchB-XGigabitEthernet0/0/3] quit
```

Configure Switch C.

```
[SwitchC-smlk-group2] flush send control-vlan 10 password simple 123
[SwitchC-smlk-group2] quit
```

Step 6 Enabling the Functions of the Smart Link Group

Configure Switch A.

```
[SwitchA] smart-link group 1
[SwitchA-smlk-group1] smart-link enable
[SwitchA-smlk-group1] quit
```

Configure Switch C.

```
[SwitchC] smart-link group 2
[SwitchC-smlk-group2] smart-link enable
[SwitchC-smlk-group2] quit
```

Step 7 Create Monitor Link groups and add the uplink and downlink interfaces to the Monitor Link groups.

Configure Switch A.

```
[SwitchA] monitor-link group 1
[SwitchA-mtlk-group1] smart-link group 1 uplink
[SwitchA-mtlk-group1] port xgigabitethernet 0/0/3 downlink 1
```

Configure Switch B.

```
[SwitchB] monitor-link group 2
[SwitchB-mtlk-group2] port xgigabitethernet 0/0/1 uplink
[SwitchB-mtlk-group2] port xgigabitethernet 0/0/3 downlink 1
```

Step 8 Set the revertive switching interval of the Monitor Link groups.

Configure Switch A.

```
[SwitchA-mtlk-group1] timer recover-time 10
[SwitchA-mtlk-group1] quit
```

Configure Switch B.

```
[SwitchB-mtlk-group2] timer recover-time 10
[SwitchB-mtlk-group2] quit
```

Step 9 Verify the configuration.

```
[SwitchA] display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Wtr-time is: 30 sec.
  There is no Load-Balance
  There is no protected-vlan reference-instance
  DeviceID: 0025-9e80-2494  Control-vlan ID: 10
      Member              Role   State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------

  XGigabitEthernet0/0/1    Master  Active    1           0000/00/00 00:00:00 UTC
+00
:00
  XGigabitEthernet0/0/2    Slave   Inactive  0           0000/00/00 00:00:00 UTC
+00
:00
[SwitchA] display monitor-link group 1
Monitor Link group 1 information :
  Recover-timer is 10 sec.
    Member              Role     State Last-up-time               Last-down-tim
e
 Smart-link1            UpLk     UP    0000/00/00 00:00:00 UTC+00:00      0000/0
0/00 00:00:00 UTC+00:00
 XGigabitEthernet0/0/3   DwLk[1]  DOWN  0000/00/00 00:00:00 UTC+00:00      0000/0
0/00 00:00:00 UTC+00:00
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
```

```
smart-link group 1
 restore enable
 smart-link enable
 port XGigabitEthernet0/0/1 master
 port XGigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
monitor-link group 1
 smart-link group 1 uplink
 port XGigabitEthernet0/0/3 downlink 1
 timer recover-time 10
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 smart-link flush receive control-vlan 10 password simple 123
#
monitor-link group 2
 port XGigabitEthernet0/0/1 uplink
 port XGigabitEthernet0/0/3 downlink 1
 timer recover-time 10
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 stp disable
#
smart-link group 2
 restore enable
 smart-link enable
 port XGigabitEthernet0/0/1 master
 port XGigabitEthernet0/0/2 slave
 timer wtr 30
 flush send control-vlan 10 password simple 123
#
return
```

7.3 RRPP Configuration

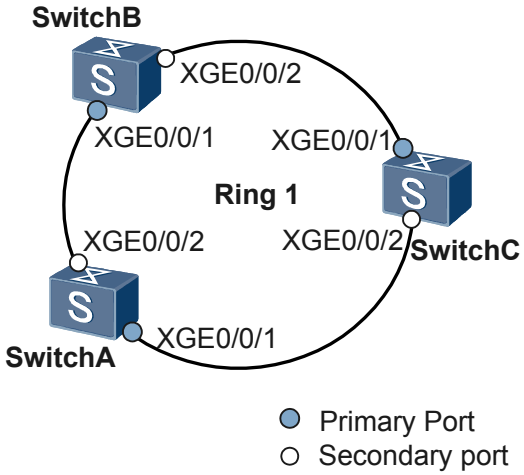
The Rapid Ring Protection Protocol (RRPP) features fast convergence, because the convergence time is irrelevant to the number of the nodes on the ring. In addition, RRPP multi-instance supports load balancing of different types of traffic.

7.3.1 Example for Configuring a Single RRPP Ring

Networking Requirements

As shown in **Figure 7-5**, Switch A, Switch B, and Switch C support the RRPP function. Switch A, Switch B, and Switch C are on ring 1 of RRPP domain 1. The data of VLANs 100 to 300 needs to be protected.

Figure 7-5 Networking diagram of a single RRPP ring



Configuration Roadmap

The configuration roadmap is as follows:

1. Map instance 1 to VLANs 100 to 300.
2. Locate Switch A, Switch B, and Switch C on ring 1 of RRPP domain 1.
3. Configure Switch A as the master node on ring 1, and configure Switch B and Switch C as transit nodes on ring 1.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of the RRPP interfaces
- Control VLAN ID of ring 1

Procedure

Step 1 Map instance 1 to VLANs 100 to 300.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 1 vlan 20 21 100 to 300
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A. The detailed configurations are omitted here.

Step 2 Create an RRPP domain and the control VLAN.

On the master node of ring 1, namely Switch A, create RRPP domain 1 and configure VLAN 20 as the main control VLAN.

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] control-vlan 20
[SwitchA-rrpp-domain-region1] quit
```

On the transit node of ring 1, namely Switch B, create RRPP domain 1 and configure VLAN 20 as the main control VLAN.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] control-vlan 20
[SwitchB-rrpp-domain-region1] quit
```

On the master node of ring 1, namely SwitchC, create RRPP domain 1 and configure VLAN 20 as the main control VLAN.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] control-vlan 20
[SwitchC-rrpp-domain-region1] quit
```

Step 3 Configure the interfaces to be added to the RRPP ring as trunk interfaces, allow VLANs 100 to 300 on the interfaces, and disable STP on the interfaces.

Configure Switch A.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[SwitchA-XGigabitEthernet0/0/1] stp disable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[SwitchA-XGigabitEthernet0/0/2] stp disable
[SwitchA-XGigabitEthernet0/0/2] quit
```

Configure Switch B.

```
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[SwitchB-XGigabitEthernet0/0/1] stp disable
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] port link-type trunk
[SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
```

```
[SwitchB-XGigabitEthernet0/0/2] stp disable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Configure Switch C.

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port link-type trunk
[SwitchC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[SwitchC-XGigabitEthernet0/0/1] stp disable
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] port link-type trunk
[SwitchC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[SwitchC-XGigabitEthernet0/0/2] stp disable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Step 4 Configure a protection VLAN and create the RRPP ring.

Configure the protection VLAN on Switch A and configure Switch A as the master node of RRPP ring 1 and specify the primary interface and secondary interface.

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchA-rrpp-domain-region1] ring 1 node-mode master primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchA-rrpp-domain-region1] ring 1 enable
[SwitchA-rrpp-domain-region1] quit
```

Configure the protection VLAN on Switch B and configure Switch B as the transit node of RRPP ring 1 and specify the primary interface and secondary interface.

```
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchB-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchB-rrpp-domain-region1] ring 1 enable
[SwitchB-rrpp-domain-region1] quit
```

Configure the protection VLAN on Switch C and configure Switch C as the transit node of RRPP ring 1 and specify the primary interface and secondary interface.

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchC-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchC-rrpp-domain-region1] ring 1 enable
[SwitchC-rrpp-domain-region1] quit
```

Step 5 Enable RRPP.

After configuring an RRPP ring, enable RRPP on each node on the ring so that the RRPP ring can be activated.

Enable RRPP on Switch A.

```
[SwitchA] rrpp enable
```

Enable RRPP on SwitchB.

```
[SwitchB] rrpp enable
```

Enable RRPP on SwitchC.

```
[SwitchC] rrpp enable
```

Step 6 Verify the configuration.

After the configurations are complete and network become stable, run the following commands to verify the configuration. Take Switch A for example.

- Run the **display rrpp brief** command on SwitchA. The following information is displayed:

```
[SwitchA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common           Secondary/Edge          Is
 ID     Level   Mode     Port                     Port
Enabled
 --------------------------------------------------------------------------
 1      0       M        XGigabitEthernet0/0/1     XGigabitEthernet0/0/2    Yes
```

  You can find that RRPP is enabled on SwitchA. The main control VLAN of domain 1 is VLAN 20 and the sub control VLAN is VLAN 21. SwitchA is the master node of ring 1. XGE 0/0/1 is the primary interface, and XGE 0/0/2 is the secondary interface.

- Run the **display rrpp verbose domain** command on SwitchA. Detailed information about RRPP domain 1 is displayed as follows:

```
[SwitchA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                          Is Active : Yes
Primary port  : XGigabitEthernet0/0/1           Port status: UP
Secondary port: XGigabitEthernet0/0/2           Port status: BLOCKED
```

----End

Configuration Files

- Configuration file of Switch A

```
sysname SwitchA
#
 vlan batch 20 to 21 100 to 300
#
 rrpp enable
#
 stp region-
configuration
  instance 1 vlan 20 to 21 100 to
300
  active region-
configuration
#
rrpp domain 1
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
```

```
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
```

- Configuration file of Switch B

```
#
sysname SwitchB
#
 vlan batch 20 to 21 100 to 300
#
 rrpp enable
#
 stp region-
configuration
  instance 1 vlan 20 to 21 100 to
300
  active region-
configuration
#
rrpp domain 1
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
#
```

- Configuration file of the SwitchC

```
#
sysname SwitchC
#
 vlan batch 20 to 21 100 to 300
#
 rrpp enable
#
 stp region-
configuration
  instance 1 vlan 20 to 21 100 to
300
  active region-
configuration
#
rrpp domain 1
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
```

```
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

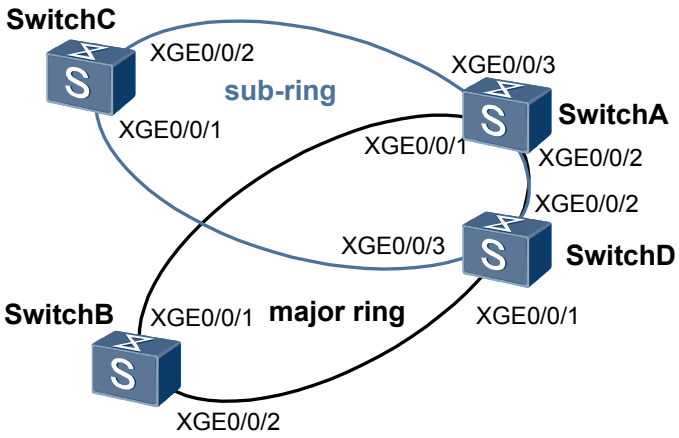
7.3.2 Example for Configuring Crossed RRPP Rings with a Single Instance

Networking Requirements

As shown in **Figure 7-6**, Switch A, Switch B, Switch C, and Switch D support the RRPP function. Switch A, Switch B, and Switch D are on ring 1 of domain 1, which is the major ring. Switch A, Switch C, and Switch D are on ring 2 of domain 1, which is the subring. Switch A is the edge node on ring 2 of domain 1, and Switch D is the assistant edge node on ring 2 of domain 1.

The main control VLAN ID is 10. The RRPP rings transmit data of VLAN 2 to VLAN 9.

Figure 7-6 Networking diagram of crossed RRPP rings with a single instance (Huawei version)



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure ring 1 (major ring) of domain 1 on Switch A, Switch B, and Switch C. Configure VLAN 10 as the main control VLAN. Add the interfaces on the major ring and subring to VLAN 2 to VLAN 9 so that the interfaces allow service packets of these VLANs to pass through.
2. Configure ring 2 (subring) of domain 1on Switch A, Switch B, and Switch D.
3. Configure Switch B as the master node of the major ring and configure Switch A andSwitch D as transit nodes of the major ring.
4. Configure Switch C as the master node of the subring; configure Switch A as the edge node of the subring; configure Switch D as the assistant edge node of the subring.

Data Preparation

To complete the configuration, you need the following data.

- Numbers of the interfaces to be added to the RRPP rings
- Control VLAN IDs and data VLAN IDs

Procedure

Step 1 Configure Switch B as the master node of the major ring.

Create data VLANs 2 to 9 on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 2 to 9
```

Configure instance 1, and map it to the VLANs allowed by the RRPP interfaces and protected VLANs.

```
[SwitchB] stp region-configuration
[SwitchB-mst-region] instance 1 vlan 2 to 11
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

On SwitchB, configure domain 1. Then configure VLAN 10 as the main control VLAN and instance 1 as the protected instance of domain 1.

```
[SwitchB] rrpp enable
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] control-vlan 10
[SwitchB-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchB-rrpp-domain-region1] quit
```

Disable STP on the interfaces to be added to the RRPP rings, configure the interfaces as trunk interfaces, and configure the interfaces to allow service packets of VLAN 2 to VLAN 9 to pass through.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchB-XGigabitEthernet0/0/1] stp disable
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] port link-type trunk
[SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchB-XGigabitEthernet0/0/2] stp disable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Configure the primary interface and secondary interface of the master node on the RRPP major ring.

```
[SwitchB] rrpp domain 1
[SwitchB-rrpp-domain-region1] ring 1 node-mode master primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchB-rrpp-domain-region1] ring 1 enable
[SwitchB-rrpp-domain-region1] quit
```

Step 2 Configure Switch C as the master node of the subring.

Create data VLANs 2 to 9 on Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 2 to 9
```

Configure instance 1, and map it to the VLANs allowed by the RRPP interfaces and protected VLANs.

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] instance 1 vlan 2 to 11
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
```

On Switch C, configure domain 1. Then configure VLAN 10 as the main control VLAN and instance 1 as the protected instance of domain 1.

```
[SwitchC] rrpp enable
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] control-vlan 10
[SwitchC-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchC-rrpp-domain-region1] quit
```

Disable STP on the interfaces to be added to the RRPP rings, configure the interfaces as trunk interfaces, and configure the interfaces to allow service packets of VLAN 2 to VLAN 9 to pass through.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port link-type trunk
[SwitchC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchC-XGigabitEthernet0/0/1] stp disable
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] port link-type trunk
[SwitchC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchC-XGigabitEthernet0/0/2] stp disable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Configure the primary interface and secondary interface of the master node on the RRPP subring.

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] ring 2 node-mode master primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 1
[SwitchC-rrpp-domain-region1] ring 2 enable
[SwitchC-rrpp-domain-region1] quit
```

Step 3 Configure Switch A as the transit node of the major ring and the edge transit node of the subring.

Create data VLANs 2 to 9 on Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 2 to 9
```

Configure instance 1, and map it to the VLANs allowed by the RRPP interfaces and protected VLANs.

```
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 1 vlan 2 to 11
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

On SwitchA, configure domain 1. Then configure VLAN 10 as the main control VLAN and instance 1 as the protected instance of domain 1.

```
[SwitchA] rrpp enable
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] control-vlan 10
[SwitchA-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchA-rrpp-domain-region1] quit
```

Disable STP on the interfaces to be added to the RRPP rings, configure the interfaces as trunk interfaces, and configure the interfaces to allow service packets of VLAN 2 to VLAN 9 to pass through.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port link-type trunk
[SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchA-XGigabitEthernet0/0/1] stp disable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] port link-type trunk
[SwitchA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchA-XGigabitEthernet0/0/2] stp disable
[SwitchA-XGigabitEthernet0/0/2] quit
[SwitchA] interface xgigabitethernet 0/0/3
[SwitchA-XGigabitEthernet0/0/3] port link-type trunk
[SwitchA-XGigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 9
[SwitchA-XGigabitEthernet0/0/3] stp disable
[SwitchA-XGigabitEthernet0/0/3] quit
```

Configure the primary interface and secondary interface of the transit node on the RRPP major ring.

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/2 secondary-port xgigabitethernet 0/0/1 level 0
[SwitchA-rrpp-domain-region1] ring 1 enable
[SwitchA-rrpp-domain-region1] quit
```

Configure the common interface and edge interface of the edge transit node on the subring.

```
[SwitchA] rrpp domain 1
[SwitchA-rrpp-domain-region1] ring 2 node-mode edge common-port xgigabitethernet
0/0/2 edge-port xgigabitethernet 0/0/3
[SwitchA-rrpp-domain-region1] ring 2 enable
[SwitchA-rrpp-domain-region1] quit
```

Step 4 Configure Switch D as the transit node of the major ring and the assistant edge node of the subring.

Create data VLANs 2 to 9 on Switch D.

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] vlan batch 2 to 9
```

Configure instance 1, and map it to the VLANs allowed by the RRPP interfaces and protected VLANs.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] instance 1 vlan 2 to 11
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

On Switch D, configure domain 1. Then configure VLAN 10 as the main control VLAN and instance 1 as the protected instance of domain 1.

```
[SwitchD] rrpp enable
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] control-vlan 10
[SwitchD-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchD-rrpp-domain-region1] quit
```

Disable STP on the interfaces to be added to the RRPP rings, configure the interfaces as trunk interfaces, and configure the interfaces to allow service packets of VLAN 2 to VLAN 9 to pass through.

```
[SwitchD] interface xgigabitethernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] port link-type trunk
[SwitchD-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 9
[SwitchD-XGigabitEthernet0/0/1] stp disable
[SwitchD-XGigabitEthernet0/0/1] quit
[SwitchD] interface xgigabitethernet 0/0/2
[SwitchD-XGigabitEthernet0/0/2] port link-type trunk
[SwitchD-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 9
[SwitchD-XGigabitEthernet0/0/2] stp disable
[SwitchD-XGigabitEthernet0/0/2] quit
[SwitchD] interface xgigabitethernet 0/0/3
[SwitchD-XGigabitEthernet0/0/3] port link-type trunk
[SwitchD-XGigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 9
[SwitchD-XGigabitEthernet0/0/3] stp disable
[SwitchD-XGigabitEthernet0/0/3] quit
```

Configure the primary interface and secondary interface of the transit node on the RRPP major ring.

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/2 secondary-port xgigabitethernet 0/0/1 level 0
[SwitchD-rrpp-domain-region1] ring 1 enable
[SwitchD-rrpp-domain-region1] quit
```

Configure the common interface and edge interface of the assistant edge node on the RRPP subring.

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] ring 2 node-mode assistant-edge common-port
xgigabitethernet 0/0/2 edge-port xgigabitethernet 0/0/3
[SwitchD-rrpp-domain-region1] ring 2 enable
[SwitchD-rrpp-domain-region1] quit
```

Step 5 Verify the configuration.

After the configurations are complete and network become stable, run the following commands to verify the configuration:

- Run the **display rrpp brief** command on Switch B. The following information is displayed:

```
[SwitchB] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 --------------------------------------------------------------------------------
 1   0          M        XGigabitEthernet0/0/1  XGigabitEthernet0/0/2  Yes
```

  You can find that RRPP is enabled on Switch B. The main control VLAN is VLAN 10, and the sub control VLAN is VLAN 11. Switch B is the master node of the major ring, with XGE 0/0/1 as the primary interface and XGE 0/0/2 as the secondary interface.

- Run the **display rrpp verbose domain** command on Switch B. The following information is displayed:

```
[SwitchB] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
```

```
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Completed
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/1         Port status: UP
Secondary port: XGigabitEthernet0/0/2         Port status: BLOCKED
```

You can find that the ring is in Complete state, and the secondary interface of the master node is blocked.

- Run the **display rrpp brief** command on SwitchC. The following information is displayed:

```
[SwitchC] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 2   1          M         XGigabitEthernet0/0/1   XGigabitEthernet0/0/2  Yes
```

The output information indicates that RRPP is enabled on SwitchC. The main control VLAN is VLAN 10, and the sub control VLAN is VLAN 11. Switch C is the master node on the subring, with XGE 0/0/1 as the primary interface and XGE 0/0/2 as the secondary interface.

- Run the **display rrpp verbose domain** command on Switch C. The following information is displayed:

```
[SwitchC] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Master
Ring State    : Completed
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/1         Port status: UP
Secondary port: XGigabitEthernet0/0/2         Port status: BLOCKED
```

You can find that the subring is in Complete state, and the secondary interface of the master node on the subring is blocked.

- Run the **display rrpp brief** command on Switch A. The following information is displayed:

```
[SwitchA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
```

```
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 1      0       T        XGigabitEthernet0/0/2  XGigabitEthernet0/0/1  Yes
 2      1       E        XGigabitEthernet0/0/2  XGigabitEthernet0/0/3  Yes
```

You can find that RRPP is enabled on Switch A. The main control VLAN is VLAN 10, and the sub control VLAN is VLAN 11. Switch A is the transit node of the major ring, with XGE 0/0/2 as the primary interface and XGE 0/0/1 as the secondary interface.

Switch A is also an edge of the subring, with XGE 0/0/2 as the common interface and XGE 0/0/3 as the edge interface.

- Run the **display rrpp verbose domain** command on Switch A. The following information is displayed:

```
[SwitchA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/2         Port status: UP
Secondary port: XGigabitEthernet0/0/1         Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : Linkup
Is Enabled    : Disable                Is Active : No
Common port   : XGigabitEthernet0/0/2         Port status: UP
Edge port     : XGigabitEthernet0/0/3         Port status: UP
```

- Run the **display rrpp brief** command on Switch D. The following information is displayed:

```
[SwitchD] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 1

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 ------------------------------------------------------------------------------
 1      0       T        XGigabitEthernet0/0/2  XGigabitEthernet0/0/1  Yes
 2      1       A        XGigabitEthernet0/0/2  XGigabitEthernet0/0/3  Yes
```

You can find that RRPP is enabled on Switch D. The main control VLAN is VLAN 10, and the sub control VLAN is VLAN 11. Switch D is the transit node of the major ring, with GXGigabitEthernet0/0/2 as the primary interface and XGigabitEthernet0/0/1 as the secondary interface. Switch D is also the assistant edge node of the major ring, with XGigabitEthernet0/0/2 as the common interface and XGigabitEthernet0/0/3 as the edge interface.

- Run the **display rrpp verbose domain** command on Switch D. The following information is displayed:

```
[SwitchD] display rrpp verbose domain 1
Domain Index  : 1
```

```
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/2         Port status: UP
Secondary port: XGigabitEthernet0/0/1         Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Assistant-edge
Ring State    : Linkup
Is Enabled    : Disable                Is Active : No
Common port   : XGigabitEthernet0/0/2         Port status: UP
Edge port     : XGigabitEthernet0/0/3         Port status: UP
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
 vlan batch 2 to 11
#
rrpp enable
#
 stp region-
configuration
  instance 1 vlan 2 to
11
  active region-
configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/2 secondary-port
XGigabitEthernet 0/0/1 level 0
 ring 1 enable
 ring 2 node-mode edge common-port XGigabitEthernet 0/0/2 edge-port
XGigabitEthernet 0/0/3
 ring 2 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

- Configuration file of Switch B

```
#
```

```
sysname SwitchB
#
 vlan batch 2 to 11
#
rrpp enable
#
 stp region-
configuration
  instance 1 vlan 2 to
11
  active region-
configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

- Configuration file of the Switch C

```
#
sysname SwitchC
#
 vlan batch 2 to 11
#
rrpp enable
#
 stp region-
configuration
  instance 1 vlan 2 to
11
  active region-
configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 1
 ring 2 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

- Configuration file of Switch D

```
#
sysname SwitchD
 vlan batch 2 to 11
```

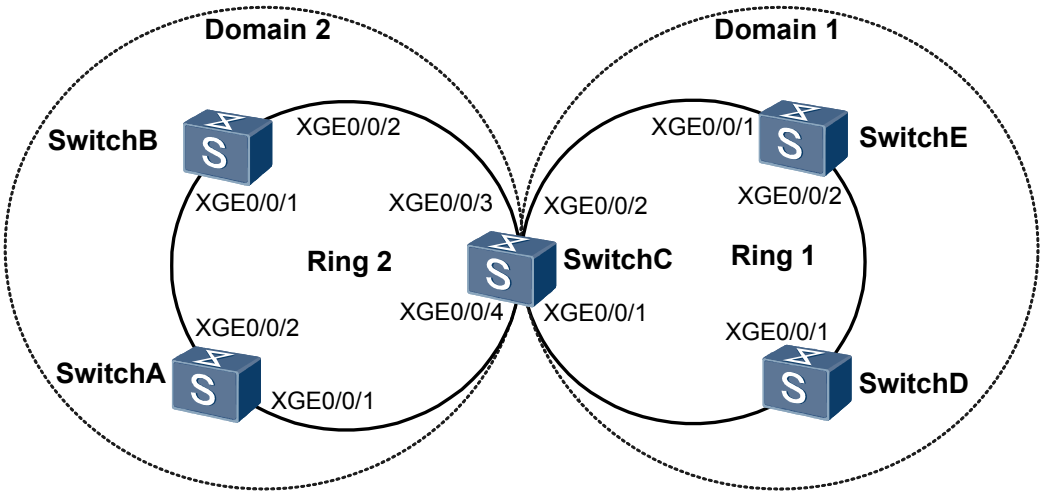
```
#
rrpp enable
#
 stp region-
configuration
  instance 1 vlan 2 to
11
  active region-
configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/2 secondary-port
XGigabitEthernet 0/0/1 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port XGigabitEthernet 0/0/2 edge-port
XGigabitEthernet 0/0/3
 ring 2 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 11
 stp disable
#
return
```

7.3.3 Example for Configuring Tangent RRPP Rings

Networking Requirements

As shown in **Figure 7-7**, Switch A, Switch B, Switch C, Switch D, and Switch E support the RRPP function. Switch A, Switch B, and Switch C are on ring 2 of domain 2. Switch C, Switch D, and Switch E are on ring 1 of domain 1. Switch C is the tangent point of the two rings.

Figure 7-7 Networking diagram of tangent RRPP rings



Configuration Roadmap

The configuration roadmap is as follows:

1. Create an instance and add the control VLANs added to the list of protected VLANs.
2. Configure ring 2 of domain 2 on Switch A, Switch B, and Switch C.
3. Configure ring 1 of domain 1 on Switch C, Switch D, and Switch E.
4. Configure Switch A as the master node on ring 2, and configure Switch B and Switch C as transit nodes on ring 2.
5. Configure Switch E as the master node on ring 1, and configure Switch C and Switch D as transit nodes on ring 1.

Data Preparation

To complete the configuration, you need the following data.

- Numbers of the RRPP interfaces
- Control VLAN IDs of ring 1 and ring 2

Procedure

Step 1 Create an instance and add the control VLANs added to the list of protected VLANs.

Configure Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] stp region-configuration
[SwitchA-mst-region] instance 2 vlan 20 to 21
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

Configure Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] stp region-configuration
[SwitchB-mst-region] instance 2 vlan 20 to 21
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
```

Configure Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] stp region-configuration
[SwitchC-mst-region] instance 1 vlan 10 to 11
[SwitchC-mst-region] instance 2 vlan 20 to 21
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
```

Configure Switch D.

```
<Quidway> system-view
[Quidway] sysname SwitchD
[SwitchD] stp region-configuration
[SwitchD-mst-region] instance 1 vlan 10 to 11
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

Configure Switch E.

```
<Quidway> system-view
[Quidway] sysname SwitchE
[SwitchE] stp region-configuration
[SwitchE-mst-region] instance 1 vlan 10 to 11
[SwitchE-mst-region] active region-configuration
[SwitchE-mst-region] quit
```

Step 2 Create RRPP domains and configure the control VLANs and protected VLANs of the domains.

Configure domain 1 on Switch E, which is the master node of ring 1. Configure VLAN 10 as the main control VLAN of domain 1, and configure the list of protected VLANs mapping instance 1.

```
[SwitchE] rrpp domain 1
[SwitchE-rrpp-domain-region1] control-vlan 10
[SwitchE-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchE-rrpp-domain-region1] quit
```

Configure domain 1 on Switch C, which is the transit node of ring 1. Configure VLAN 10 as the main control VLAN of domain 1, and configure the list of protected VLANs mapping instance 1.

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] control-vlan 10
[SwitchC-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchC-rrpp-domain-region1] quit
```

Configure domain 1 on Switch D, which is the transit node of ring 1. Configure VLAN 10 as the main control VLAN of domain 1, and configure the list of protected VLANs of instance 1.

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] control-vlan 10
[SwitchD-rrpp-domain-region1] protected-vlan reference-instance 1
[SwitchD-rrpp-domain-region1] quit
```

Configure domain 2 on Switch E, which is the master node of ring 2. Configure VLAN 20 as the main control VLAN of domain 2, and configure the list of protected VLANs mapping instance 1.

```
[SwitchA] rrpp domain 2
[SwitchA-rrpp-domain-region2] control-vlan 20
[SwitchA-rrpp-domain-region2] protected-vlan reference-instance 2
[SwitchA-rrpp-domain-region2] quit
```

Configure domain 2 on Switch B, which is the transit node of ring 2. Configure VLAN 20 as the main control VLAN of domain 2, and configure the list of protected VLANs of instance 2.

```
[SwitchB] rrpp domain 2
[SwitchB-rrpp-domain-region2] control-vlan 20
[SwitchB-rrpp-domain-region2] protected-vlan reference-instance 2
[SwitchB-rrpp-domain-region2] quit
```

Configure domain 2 on Switch C, which is the transit node of ring 2. Configure VLAN 20 as the main control VLAN of domain 2, and configure the list of protected VLANs of instance 2.

```
[SwitchC] rrpp domain 2
[SwitchC-rrpp-domain-region2] control-vlan 20
[SwitchC-rrpp-domain-region2] protected-vlan reference-instance 2
[SwitchC-rrpp-domain-region2] quit
```

Step 3 Set the timers of the RRPP domains

NOTE

You can set two timers for the tangent point because the two tangent rings reside in different domains.

Set the Hold timer and Fail timer for Switch E, the master node on ring 1.

```
[SwitchE] rrpp domain 1
[SwitchE-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
[SwitchE-rrpp-domain-region1] quit
```

Set the Hold timer and Fail timer for Switch D, the transit node on ring 1.

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
[SwitchD-rrpp-domain-region1] quit
```

Set the Hold timer and Fail timer for Switch C, the transit node on ring 1.

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
[SwitchC-rrpp-domain-region1] quit
```

Set the Hold timer and Fail timer for Switch A, the master node on ring 2.

```
[SwitchA] rrpp domain 2
[SwitchA-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
[SwitchA-rrpp-domain-region2] quit
```

Set the Hold timer and Fail timer for Switch B, the transit node on ring 2.

```
[SwitchB] rrpp domain 2
[SwitchB-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
[SwitchB-rrpp-domain-region2] quit
```

Set the Hold timer and Fail timer for Switch C, the transit node on ring 2.

```
[SwitchC] rrpp domain 2
[SwitchC-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
[SwitchC-rrpp-domain-region2] quit
```

Step 4 Disable STP on the interfaces to be added to the RRPP rings.

Disable STP on the interfaces to be added to the RRPP ring on Switch A.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] stp disable
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface xgigabitethernet 0/0/2
[SwitchA-XGigabitEthernet0/0/2] stp disable
[SwitchA-XGigabitEthernet0/0/2] quit
```

Disable STP on the interfaces to be added to the RRPP ring on Switch B.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] stp disable
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] stp disable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Disable STP on the interfaces to be added to the RRPP ring on Switch C.

```
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] stp disable
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] stp disable
[SwitchC-XGigabitEthernet0/0/2] quit
[SwitchC] interface xgigabitethernet 0/0/3
[SwitchC-XGigabitEthernet0/0/1] stp disable
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface xgigabitethernet 0/0/4
[SwitchC-XGigabitEthernet0/0/2] stp disable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Disable STP on the interfaces to be added to the RRPP ring on Switch E.

```
[SwitchE] interface xgigabitethernet 0/0/1
[SwitchE-XGigabitEthernet0/0/1] stp disable
[SwitchE-XGigabitEthernet0/0/1] quit
[SwitchE] interface xgigabitethernet 0/0/2
[SwitchE-XGigabitEthernet0/0/2] stp disable
[SwitchE-XGigabitEthernet0/0/2] quit
```

Disable STP on the interfaces to be added to the RRPP ring on Switch D.

```
[SwitchD] interface xgigabitethernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] stp disable
[SwitchD-XGigabitEthernet0/0/1] quit
[SwitchD] interface xgigabitethernet 0/0/2
[SwitchD-XGigabitEthernet0/0/2] stp disable
[SwitchD-XGigabitEthernet0/0/2] quit
```

Step 5 Create RRPP rings.

Configure nodes on ring 2. The configuration procedure is as follows:

Configure Switch A as the master node of ring 2 and specify the primary and secondary interfaces.

```
[SwitchA] rrpp domain 2
[SwitchA-rrpp-domain-region2] ring 2 node-mode master primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchA-rrpp-domain-region2] ring 2 enable
[SwitchA-rrpp-domain-region2] quit
```

Configure SwitchB as a transit node of ring 2 (major ring) and specify the primary and secondary interfaces.

```
[SwitchB] rrpp domain 2
[SwitchB-rrpp-domain-region2] ring 2 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchB-rrpp-domain-region2] ring 2 enable
[SwitchB-rrpp-domain-region2] quit
```

Configure Switch C as a transit node of RRPP ring 2 and specify the primary and secondary interfaces.

```
[SwitchC] rrpp domain 2
[SwitchC-rrpp-domain-region2] ring 2 node-mode transit primary-port
xgigabitethernet 0/0/3 secondary-port xgigabitethernet 0/0/4 level 0
[SwitchC-rrpp-domain-region2] ring 2 enable
[SwitchC-rrpp-domain-region2] quit
```

Configure nodes on ring 1. The configuration procedure is as follows:

Configure Switch E as the master node of ring 1 (major ring) and specify the primary and secondary interfaces.

```
[SwitchE] rrpp domain 1
[SwitchE-rrpp-domain-region1] ring 1 node-mode master primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchE-rrpp-domain-region1] ring 1 enable
[SwitchE-rrpp-domain-region1] quit
```

Configure Switch C as a transit node of ring 1 and specify the primary and secondary interfaces.

```
[SwitchC] rrpp domain 1
[SwitchC-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchC-rrpp-domain-region1] ring 1 enable
[SwitchC-rrpp-domain-region1] quit
```

Configure Switch D as a transit node of ring 1 and specify the primary and secondary interfaces.

```
[SwitchD] rrpp domain 1
[SwitchD-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[SwitchD-rrpp-domain-region1] ring 1 enable
[SwitchD-rrpp-domain-region1] quit
```

Step 6 Enable RRPP.

After configuring an RRPP ring, enable RRPP on each node on the ring. Then the RRPP ring can be activated.

Enable RRPP on Switch A.

```
[SwitchA] rrpp enable
```

Enable RRPP on Switch B.

```
[SwitchB] rrpp enable
```

Enable RRPP on Switch C.

```
[SwitchC] rrpp enable
```

Enable RRPP on Switch E.

```
[SwitchE] rrpp enable
```

Enable RRPP on Switch D.

```
[SwitchD] rrpp enable
```

Step 7 Verify the configuration.

After the configurations are complete and network become stable, run the following commands to verify the configuration. Take the tangent point Switch C for example.

- Run the **display rrpp brief** command on Switch C. The following information is displayed:

```
[SwitchC] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 2 sec(default is 1 sec)  Fail Timer : 7 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 --------------------------------------------------------------------------
 1      0       T        XGigabitEthernet0/0/1  XGigabitEthernet0/0/2  Yes
Domain Index  : 2
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 2
Hello Timer   : 3 sec(default is 1 sec)  Fail Timer : 10 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common        Secondary/Edge        Is
 ID     Level   Mode     Port                  Port                  Enabled
 --------------------------------------------------------------------------
 2      0       T        XGigabitEthernet0/0/3  XGigabitEthernet0/0/4  Yes
```

  You can find that RRPP is enabled on Switch C. The main control VLAN of domain 1 is VLAN 10 and the sub control VLAN is VLAN 11. Switch C is the master node of ring 1, with XGE 0/0/1 as the primary interface and XGE 0/0/2 as the secondary interface.

The main control VLAN of domain 2 is VLAN 20, and the sub control VLAN is VLAN 21. Switch C is a transit node on ring 2, with XGE 0/0/3 as the primary interface and XGE 0/0/4 as the secondary interface.

- Run the **display rrpp verbose domain** command on Switch C to view the domain information.

  # View detailed information about domain 1.

```
[SwitchC] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 10    sub 11
Protected VLAN : Reference Instance 1
Hello Timer   : 2 sec(default is 1 sec)  Fail Timer : 7 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/1         Port status: UP
Secondary port: XGigabitEthernet0/0/2         Port status: UP
```

  # View detailed information about domain 2.

```
[SwitchC] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 20    sub 21
Protected VLAN : Reference Instance 2
Hello Timer   : 3 sec(default is 1 sec)  Fail Timer : 10 sec(default is 6 sec)

RRPP Ring     : 2
Ring Level    : 0
Node Mode     : Transit
Ring State    : Linkup
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/3         Port status: UP
Secondary port: XGigabitEthernet0/0/4         Port status: UP
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
vlan batch 20 to 21
#
rrpp enable
#
 stp region-
configuration
  instance 2 vlan 20 to
21
  active region-configuration
#
rrpp domain 2
 control-vlan 20
 protected-vlan reference-instance 2
 timer hello-timer 3 fail-timer 10
 ring 2 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 2 enable
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 20 to 21
 stp disable
#
```

```
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 to 21
 stp disable
#
```

- Configuration file of SwitchB

```
#
sysname Switch B
#
vlan batch 20 to 21
#
rrpp enable
#
 stp region-
configuration
  instance 2 vlan 20 to
21
  active region-configuration
#
rrpp domain 2
 control-vlan 20
 protected-vlan reference-instance 2
 timer hello-timer 3 fail-timer 10
 ring 2 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 2 enable
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 20 to 21
 stp disable
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 20 to 21
 stp disable
#
return
#
```

- Configuration file of the Switch C

```
#
sysname SwitchC
#
vlan batch 10 to 11 20 to 21
#
rrpp enable
#
 stp region-
configuration
  instance 1 vlan 10 to 11
  instance 2 vlan 20 to
21
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 timer hello-timer 2 fail-timer 7
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 20
 protected-vlan reference-instance 2
 timer hello-timer 3 fail-timer 10
 ring 2 node-mode transit primary-port XGigabitEthernet 0/0/3 secondary-port
XGigabitEthernet 0/0/4 level 0
 ring 2 enable
#
interface XGigabitEthernet 0/0/1
```

```
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface XGigabitEthernet 0/0/2
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface XGigabitEthernet 0/0/3
 port hybrid tagged vlan 20 to 21
 stp disable
#
interface XGigabitEthernet 0/0/4
 port hybrid tagged vlan 20 to 21
 stp disable
#
return
```

- Configuration file of Switch D

```
#
sysname SwitchD
#
vlan batch 10 to 11
#
 rrpp enable
#
 stp region-
configuration
  instance 1 vlan 10 to
11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 timer hello-timer 2 fail-timer 7
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface XGigabitEthernet0/0/2
 port hybrid tagged vlan 10 to 11
 stp disable
#
return
```

- Configuration file of Switch E

```
#
sysname SwitchE
#
vlan batch 10 to 11
#
rrpp enable
#
 stp region-
configuration
  instance 1 vlan 10 to
11
  active region-configuration
#
rrpp domain 1
 control-vlan 10
 protected-vlan reference-instance 1
 timer hello-timer 2 fail-timer 7
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
```

```
#
interface XGigabitEthernet 0/0/1
 port hybrid tagged vlan 10 to 11
 stp disable
#
interface XGigabitEthernet 0/0/2
 port hybrid tagged vlan 10 to 11
 stp disable
#
return
```

7.3.4 Example for Configuring a Single RRPP Ring with Multiple Instances

Networking Requirements

As shown in **Figure 7-8**, UPE A, UPE B, UPE C, and PE-AGG form a multi-instance RRPP ring.

Two rings are involved in the networking, ring 1 in domain 1 and ring 1 in domain 2.

VLANs 100 to 300 are configured on CE. Domain 1 and domain 2 share the traffic of packets from VLANs 100 to 300. Packets from VLANs 100 to 200 are transmitted through domain 1, and packets from VLANs 201 to 300 are transmitted through domain 2.

Table 7-1 shows the mapping between protected VLANs and instances in domain 1 and domain 2.

Table 7-1 Mapping between protected VLANs and instances

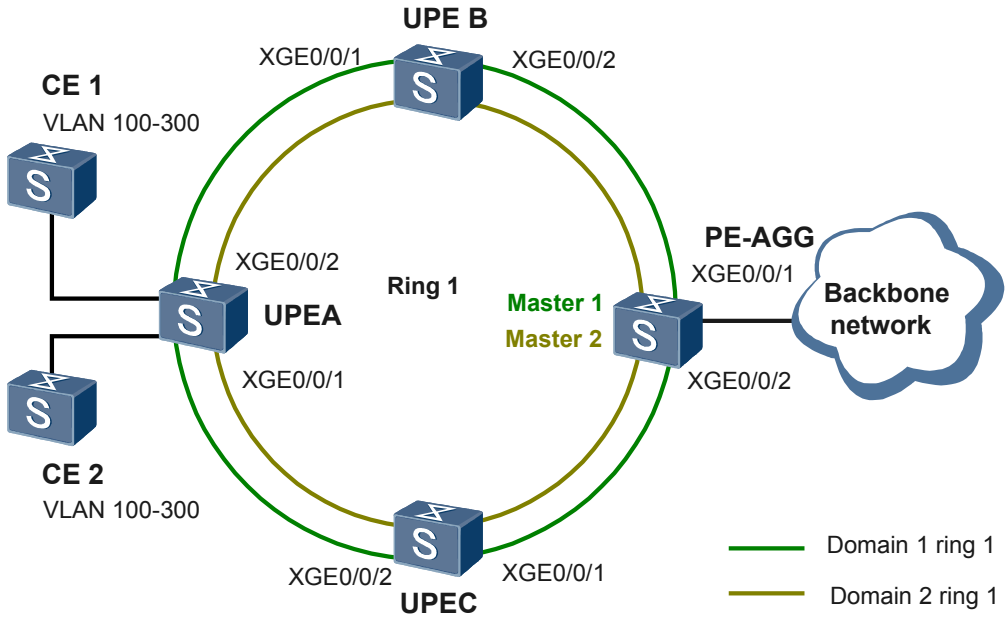
Ring ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
Domain 1	VLAN 5, VLAN 6	Instance 1	VLAN 100-200	Instance 1
Domain 2	VLAN 10, VLAN 11	Instance 2	VLAN 201-300	Instance 2

Table 7-2 shows the master node of each ring, and the primary port and secondary port on the master node.

Table 7-2 Master nodes, and primary and secondary ports on the master nodes

Ring ID	Master Node	Primary Port	Secondary Port
Ring 1 in domain 1	PE-AGG	XGE0/0/1	XGE0/0/2
Ring 1 in domain 2	PE-AGG	XGE0/0/2	XGE0/0/1

Figure 7-8 Networking diagram of single RRPP ring with multiple instances



Configuration Roadmap

The configuration roadmap is as follows:

1. Map instance 1 to VLANs 100 to 200. Map instance 2 to VLANs 201 to 300.
2. Add UPE A, UPE B, UPE C, and PE-AGG to ring 1 in domain 1.
3. Add UPE A, UPE B, UPE C, and PE-AGG to ring 1 in domain 2.
4. Configure protected VLANs in domain 1 and domain 2.
5. Configure control VLANs in domain 1 and domain 2.
6. Configure PE-AGG as the master node on ring 1 in domain 1 and configure UPE A, UPE B, and UPE C as transit nodes.
7. Configure PE-AGG as the master node on ring 1 in domain 2 and configure UPE A, UPE B, and UPE C as transit nodes.

Data Preparation

To complete the configuration, you need the following data:

- Instance IDs
- Range of the protected VLANs
- IDs of the control VLANs
- Numbers of the RRPP interfaces

Procedure

Step 1 Create instances.

- Configure UPE A.

Create data VLANs 100 to 300 on UPE A.

```
<Quidway> system-view
[Quidway] sysname UPEA
[UPEA] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPEA-mst-region] active region-configuration
[UPEA-mst-region] quit
```

- # Configure UPE B.

Create data VLANs 100 to 300 on UPE B.

```
<Quidway> system-view
[Quidway] sysname UPEB
[UPEB] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPEB-mst-region] active region-configuration
[UPEB-mst-region] quit
```

- Configure UPE C.

Create data VLANs 100 to 300 on UPE C.

```
<Quidway> system-view
[Quidway] sysname UPEC
[UPEC] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPEC-mst-region] active region-configuration
[UPEC-mst-region] quit
```

- Configure PE-AGG.

Create data VLANs 100 to 300 on PE-AGG.

```
<Quidway> system-view
[Quidway] sysname PE-AGG
[PE-AGG] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[PE-AGG] stp region-configuration
[PE-AGG-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[PE-AGG-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[PE-AGG-mst-region] active region-configuration
[PE-AGG-mst-region] quit
```

- Verify the configuration.

Run the **display stp region-configuration** command on the devices to view the mapping between instances and VLANs. The displayed information on UPE A is as follows:

```
[UPEA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0cd568d00
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
      1       5 to 6, 100 to 200
      2       10 to 11, 201 to 300
```

Step 2 Configure RRPP interfaces.

- Configure UPE A.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE A. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEA] interface xgigabitethernet 0/0/1
[UPEA-XGigabitEthernet0/0/1] port link-type trunk
[UPEA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-XGigabitEthernet0/0/1] stp disable
[UPEA-XGigabitEthernet0/0/1] quit
[UPEA] interface xgigabitethernet 0/0/2
[UPEA-XGigabitEthernet0/0/2] port link-type trunk
[UPEA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-XGigabitEthernet0/0/2] stp disable
[UPEA-XGigabitEthernet0/0/2] quit
```

- # Configure UPE B.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE B. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEB] interface xgigabitethernet 0/0/1
[UPEB-XGigabitEthernet0/0/1] port link-type trunk
[UPEB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
```

```
[UPEB-XGigabitEthernet0/0/1] stp disable
[UPEB-XGigabitEthernet0/0/1] quit
[UPEB] interface xgigabitethernet 0/0/2
[UPEB-XGigabitEthernet0/0/2] port link-type trunk
[UPEB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-XGigabitEthernet0/0/2] stp disable
[UPEB-XGigabitEthernet0/0/2] quit
```

- Configure UPE C.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE C. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEC] interface xgigabitethernet 0/0/1
[UPEC-XGigabitEthernet0/0/1] port link-type trunk
[UPEC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/1] stp disable
[UPEC-XGigabitEthernet0/0/1] quit
[UPEC] interface xgigabitethernet 0/0/2
[UPEC-XGigabitEthernet0/0/2] port link-type trunk
[UPEC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/2] stp disable
[UPEC-XGigabitEthernet0/0/2] quit
```

- Configure PE-AGG.

Disable STP of the interfaces that need to be added to the RRPP ring on PE-AGG. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[PE-AGG] interface xgigabitethernet 0/0/1
[PE-AGG-XGigabitEthernet0/0/1] port link-type trunk
[PE-AGG-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-XGigabitEthernet0/0/1] stp disable
[PE-AGG-XGigabitEthernet0/0/1] quit
[PE-AGG] interface xgigabitethernet 0/0/2
[PE-AGG-XGigabitEthernet0/0/2] port link-type trunk
[PE-AGG-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-XGigabitEthernet0/0/2] stp disable
[PE-AGG-XGigabitEthernet0/0/2] quit
```

Step 3 Create RRPP domains and configure the protected VLANs and control VLANs.

- Configure UPE A.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 5
[UPEA-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- # Configure UPE B.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 5
[UPEB-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 5
[UPEC-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- Configure PE-AGG.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 5
[PE-AGG-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] protected-vlan reference-instance 2
[PE-AGG-rrpp-domain-region2] control-vlan 10
[PE-AGG-rrpp-domain-region2] quit
```

Step 4 Create RRPP rings.

- Configure UPE A.

Configure UPE A as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE A.

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

Configure UPE A as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE A.

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- # Configure UPE B.

Configure UPE B as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE B.

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

Configure UPE B as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE B.

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

Configure UPE C as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE C.

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

Configure UPE C as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE C.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

- Configure PE-AGG.

Configure PE-AGG as the master node of ring 1 in domain 1. Configure XGE 0/0/1 as the primary port and XGE 0/0/2 as the secondary port.

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

Configure PE-AGG as the master node of ring 1 in domain 2. Configure XGE 0/0/2 as the primary port and XGE 0/0/1 as the secondary port.

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] ring 1 node-mode master primary-port xgigabitethernet
0/0/2 secondary-port xgigabitethernet 0/0/1 level 0
[PE-AGG-rrpp-domain-region2] ring 1 enable
[PE-AGG-rrpp-domain-region2] quit
```

Step 5 Enable the RRPP protocol.

After configuring an RRPP ring, you need to enable RRPP on each node on the ring to activate the RRPP ring. The configuration procedure is as follows:

- Configure UPE A.

Enable the RRPP protocol.

```
[UPEA] rrpp enable
```

- # Configure UPE B.

Enable the RRPP protocol.

```
[UPEB] rrpp enable
```

- Configure UPE C.

Enable the RRPP protocol.

```
[UPEC] rrpp enable
```

- Configure PE-AGG.

Enable the RRPP protocol.

```
[PE-AGG] rrpp enable
```

Step 6 Verify the configuration.

After the preceding configurations are complete and the network topology becomes stable, perform the following operations to verify the configuration. Here, UPE A and PE-AGG are used as examples.

- Run the **display rrpp brief** command on UPE A. The following information is displayed:

```
[UPEA] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 2

Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 --------------------------------------------------------------------------
 1     0      T     XGigabitEthernet0/0/1     XGigabitEthernet0/0/2     Yes

Domain Index   : 2
Control VLAN   : major 10    sub 11
Protected VLAN : Reference Instance 2
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 --------------------------------------------------------------------------
 1     0      T     XGigabitEthernet0/0/1     XGigabitEthernet0/0/2     Yes
```

You can see that the RRPP protocol is enabled on UPE A.

In domain 1, VLAN 5 is the control VLAN; VLANs mapping instance 1 are the protected VLANs; UPE A is a transit node on ring 1. The primary port is XGE 0/0/1, and the secondary port is XGE 0/0/2.

In domain 2, VLAN 10 is the control VLAN; VLANs mapping instance 2 are the protected VLANs; UPE A is a transit node on ring 1. The primary port is XGE 0/0/1, and the secondary port is XGE 0/0/2.

- Run the **display rrpp brief** command on PE-AGG. The following information is displayed:

```
[PE-AGG] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge
```

```
RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port                    Enabled
 ------------------------------------------------------------------------------
 1      0       M         XGigabitEthernet0/0/1    XGigabitEthernet0/0/2    Yes

Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common           Secondary/Edge          Is
 ID     Level   Mode     Port                     Port                    Enabled
 ------------------------------------------------------------------------------
 1      0        M         XGigabitEthernet0/0/2    XGigabitEthernet0/0/1   Yes
```

The preceding information shows that the RRPP protocol is enabled on PE-AGG.

In domain 1, VLAN 5 is the control VLAN; VLANs mapping instance 1 are the protected VLANs; PE-AGG is the master node on ring 1. The primary port is XGE 0/0/1, and the secondary port is XGE 0/0/2.

In domain 2, VLAN 10 is the control VLAN; VLANs mapping instance 2 are the protected VLANs; PE-AGG is the master node on ring 1. The primary port is XGE 0/0/2, and the secondary port is XGE0/0/1.

- Run the **display rrpp verbose domain** command on UPE A. You can obtain the following results:

View detailed information about UPE A in domain 1.

```
[UPEA] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/1         Port status: UP
Secondary port: XGigabitEthernet0/0/2         Port status: UP
```

The preceding information shows that VLAN 5 is the control VLAN in domain 1 and VLANs mapping instance 1 are the protected VLANs. UPE A is a transit node in domain 1 and is in LinkUp state.

View detailed information about UPE A in domain 2.

```
[UPEA] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
```

```
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/1         Port status: UP
Secondary port: XGigabitEthernet0/0/2         Port status: UP
```

The preceding information shows that VLAN 10 is the control VLAN in domain 2, and VLANs mapping instance 2 are the protected VLANs. UPE A is a transit node in domain 2 and is in LinkUp state.

- Run the **display rrpp verbose domain** command on PE-AGG. You can obtain the following results:

View detailed information about PE-AGG in domain 1.

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/1         Port status: UP
Secondary port: XGigabitEthernet0/0/2         Port status: BLOCKED
```

The preceding information shows that VLAN 5 is the control VLAN in domain 1 and VLANs mapping instance 1 are the protected VLANs.

PE-AGG is the master node in domain 1 and is in Complete state.

The primary port is XGE 0/0/1, and the secondary port is XGE 0/0/2.

View detailed information about PE-AGG in domain 2.

```
[PE-AGG] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                Is Active : Yes
Primary port  : XGigabitEthernet0/0/2         Port status: UP
Secondary port: XGigabitEthernet0/0/1         Port status: BLOCKED
```

The preceding information shows that VLAN 10 is the control VLAN in domain 2, and VLANs mapping instance 2 are the protected VLANs.

PE-AGG is the master node in domain 2 and is in Complete state.

The primary port is XGE 0/0/2, and the secondary port is XGE 0/0/1.

----End

Configuration Files

- Configuration file of UPE A

```
#
sysname UPEA
```

```
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE B

```
#
sysname UPEB
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
```

```
#
return
```

- Configuration file of UPE C

```
#
sysname UPEC
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of PE-AGG

```
#
sysname PE-AGG
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
protected-vlan reference-instance 2
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/2 secondary-
portXGigabitEthernet 0/0/1 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
```

```
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

7.3.5 Example for Configuring Crossed RRPP Rings with Multiple Instances (HW version)

Networking Requirements

As shown in **Figure 7-9**, UPE A, UPE B, UPE C, UPE D, and PE-AGG form two multi-instance major rings: ring 1 in domain 1 and ring 1 in domain 2.

CE1, UPE B, and UPE C form two subrings: ring 2 in domain 1 and ring 2 in domain 2. CE1 is connected to the major rings through XGE 0/0/3 of UPE B and XGE 0/0/3 of UPE C. UPE B is an edge node, and UPE is an assistant edge node.

CE2, UPE B, and UPE C form two subrings: ring 3 in domain 1 and ring 3 in domain 2. CE2 is connected to the major rings through XGE 0/0/4 of UPE B and XGE 0/0/4 of UPE C. UPE B is an edge node, and UPE is an assistant edge node.

VLANs 100 to 300 are configured on CE. Domain 1 and domain 2 share the traffic of packets from VLANs 100 to 300. Packets from VLANs 100 to 200 are transmitted through domain 1, and packets from VLANs 201 to 300 are transmitted through domain 2.

Table 7-3 shows the mapping between protected VLANs and instances in domain 1 and domain 2.

Table 7-3 Mapping between protected VLANs and instances

Domain ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
Domain 1	VLAN 5, VLAN 6	Instance 1	VLAN 100-200	Instance 1
Domain 2	VLAN 10, VLAN 11	Instance 2	VLAN 201-300	Instance 2

Table 7-4 shows the master node of each ring, and the primary port and secondary port on each master node.

Table 7-4 Master nodes, and primary and secondary ports on the master nodes

Ring ID	Master Node	Primary Port	Secondary Port	Ring Type
Ring 1 in domain 1	PE-AGG	XGE 0/0/1	XGE 0/0/2	Major ring

Ring ID	Master Node	Primary Port	Secondary Port	Ring Type
Ring 1 in domain 2	PE-AGG	XGE 0/0/2	XGE 0/0/1	Major ring
Ring 2 in domain 1	CE1	XGE 0/0/1	XGE 0/0/2	Sub ring
Ring 2 in domain 2	CE1	XGE 0/0/2	XGE 0/0/1	Sub ring
Ring 3 in domain 1	CE2	XGE 0/0/1	XGE 0/0/2	Sub ring
Ring 3 in domain 2	CE2	XGE 0/0/2	XGE 0/0/1	Sub ring

Table 7-5 shows the edge nodes, assistant edge nodes, public port, and edge port of the subrings.

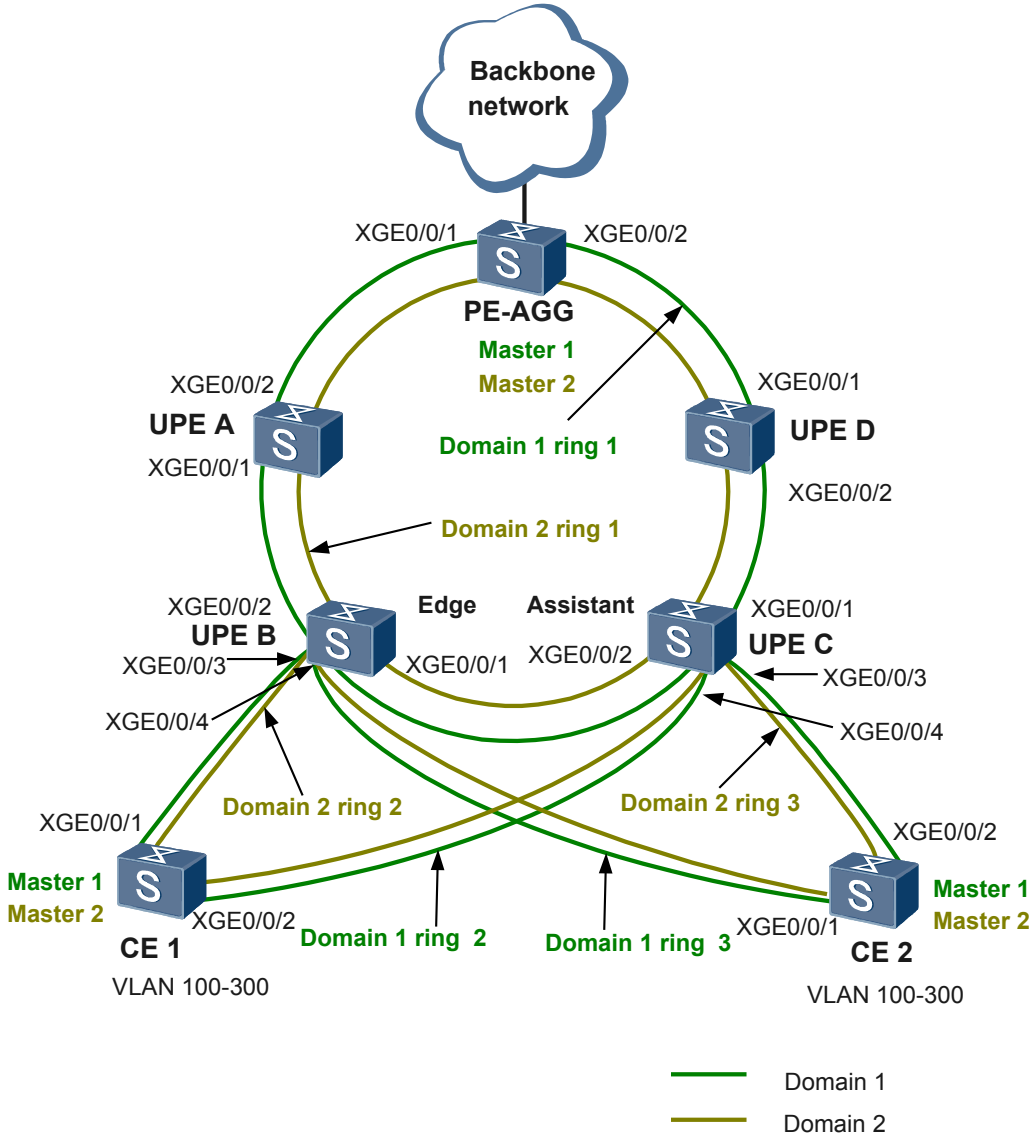
Table 7-5 Edge nodes, assistant edge nodes, public port, and edge port of the subrings

Ring ID	Edge Node	Common Port	Edge Port	Edge-Assistant Node	Common Port	Edge Port
Ring 2 in domain 1	UPE B	XGE 0/0/1	XGE 0/0/3	UPE C	XGE 0/0/2	XGE 0/0/3
Ring 3 in domain 1	UPE B	XGE 0/0/1	XGE 0/0/4	UPE C	XGE 0/0/2	XGE 0/0/4
Ring 2 in domain 2	UPE B	XGE 0/0/1	XGE 0/0/3	UPE C	XGE 0/0/2	XGE 0/0/3
Ring 3 in domain 2	UPE B	XGE 0/0/1	XGE 0/0/4	UPE C	XGE 0/0/2	XGE 0/0/4

To reduce the Edge-Hello packets sent on the major ring and increase available bandwidth, you can add the four subrings to a ring group.

To prevent topology flapping, you need to set the Link-Up timer on the master nodes.

Figure 7-9 Networking diagram of crossed RRPP rings with multiple instances



Configuration Roadmap

The configuration roadmap is as follows:

1. Map instance 1 to VLANs 100 to 200. Map instance 2 to VLANs 201 to 300.
2. Add UPE A, UPE B, UPE C, UPE D, and PE-AGG to ring 1 in domain 1 and ring 1 in domain 2.
3. Add CE1, UPE B, and UPE C to ring 2 in domain 1 and ring 2 in domain 2.
4. Add CE2, UPE B, and UPE C to ring 3 in domain 1 and ring 3 in domain 2.
5. Configure protected VLANs in domain 1 and domain 2.
6. Configure control VLANs in domain 1 and domain 2.

7. Configure PE-AGG as the master node and configure UPE A, UPE B, and UPE C as transit nodes on ring 1 in domain 1 and ring 1 in domain 2.
8. Configure CE1 as the master node and configure UPE B and UPE C as transit nodes on ring 2 in domain 1 and ring 2 in domain 2.
9. Configure CE2 as the master node and configure UPE B and UPE C as transit nodes on ring 3 in domain 1 and ring 3 in domain 2.
10. Configure a ring group.
11. Set the link-Up timer.

Data Preparation

To complete the configuration, you need the following data:

- Instance IDs
- Range of the protected VLANs
- IDs of the control VLANs
- Numbers of the RRPP interfaces
- ID of the ring group
- Link-Up-Delay timer

Procedure

Step 1 Create instances.

- Configure CE1.

  # Create data VLANs 100 to 300 on CE1.

  ```
  <Quidway> system-view
  [Quidway] sysname CE1
  [CE1] vlan batch 100 to 300
  ```

  # Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

  ```
  [CE1] stp region-configuration
  [CE1-mst-region] instance 1 vlan 5 6 100 to 200
  ```

  # Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

  ```
  [CE1-mst-region] instance 2 vlan 10 11 201 to 300
  ```

  # Activate the configuration.

  ```
  [CE1-mst-region] active region-configuration
  [CE1-mst-region] quit
  ```

- Configure CE2.

  # Create data VLANs 100 to 300 on CE2.

  ```
  <Quidway> system-view
  [Quidway] sysname CE2
  [CE2] vlan batch 100 to 300
  ```

  # Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

  ```
  [CE2] stp region-configuration
  [CE2-mst-region] instance 1 vlan 5 6 100 to 200
  ```

  # Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[CE2-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[CE2-mst-region] active region-configuration
[CE2-mst-region] quit
```

- Configure UPE A.

  # Create data VLANs 100 to 300 on UPE A.

```
<Quidway> system-view
[Quidway] sysname UPEA
[UPEA] vlan batch 100 to 300
```

  # Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 5 6 100 to 200
```

  # Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

  # Activate the configuration.

```
[UPEA-mst-region] active region-configuration
[UPEA-mst-region] quit
```

- # Configure UPE B.

  # Create data VLANs 100 to 300 on UPE B.

```
<Quidway> system-view
[Quidway] sysname UPEB
[UPEB] vlan batch 100 to 300
```

  # Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 5 6 100 to 200
```

  # Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

  # Activate the configuration.

```
[UPEB-mst-region] active region-configuration
[UPEB-mst-region] quit
```

- Configure UPE C.

  # Create data VLANs 100 to 300 on UPE C.

```
<Quidway> system-view
[Quidway] sysname UPEC
[UPEC] vlan batch 100 to 300
```

  # Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 5 6 100 to 200
```

  # Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

  # Activate the configuration.

```
[UPEC-mst-region] active region-configuration
[UPEC-mst-region] quit
```

- Configure UPE D.

Create data VLANs 100 to 300 on UPE D.

```
<Quidway> system-view
[Quidway] sysname UPED
[UPED] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPED] stp region-configuration
[UPED-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPED-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPED-mst-region] active region-configuration
[UPED-mst-region] quit
```

- Configure PE-AGG.

  # Create data VLANs 100 to 300 on PE-AGG.

  ```
  <Quidway> system-view
  [Quidway] sysname PE-AGG
  [PE-AGG] vlan batch 100 to 300
  ```

  # Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

  ```
  [PE-AGG] stp region-configuration
  [PE-AGG-mst-region] instance 1 vlan 5 6 100 to 200
  ```

  # Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

  ```
  [PE-AGG-mst-region] instance 2 vlan 10 11 201 to 300
  ```

  # Activate the configuration.

  ```
  [PE-AGG-mst-region] active region-configuration
  [PE-AGG-mst-region] quit
  ```

- Verify the configuration.

  View the mapping between instances and VLANs. The displayed information on UPE A is as follows:

  ```
  [UPEA] display stp region-configuration
   Oper configuration
     Format selector    :0
     Region name        :00e0cd568d00
     Revision level     :0

     Instance   Vlans Mapped
     0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
     1       5 to 6, 100 to 200
     2       10 to 11, 201 to 300
  ```

Step 2 Configure RRPP interfaces.

- Configure CE1.

  # Disable STP on the interfaces that need to be added to the RRPP ring on CE1. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

  ```
  [CE1] interface xgigabitethernet 0/0/1
  [CE1-XGigabitEthernet0/0/1] port link-type trunk
  [CE1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
  [CE1-XGigabitEthernet0/0/1] stp disable
  [CE1-XGigabitEthernet0/0/1] quit
  [CE1] interface xgigabitethernet 0/0/2
  [CE1-XGigabitEthernet0/0/2] port link-type trunk
  [CE1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
  ```

```
[CE1-XGigabitEthernet0/0/2] stp disable
[CE1-XGigabitEthernet0/0/2] quit
```

- Configure CE2.

  # Disable STP on the interfaces that need to be added to the RRPP ring on CE2. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[CE2] interface xgigabitethernet 0/0/1
[CE2-XGigabitEthernet0/0/1] port link-type trunk
[CE2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[CE2-XGigabitEthernet0/0/1] stp disable
[CE2-XGigabitEthernet0/0/1] quit
[CE2] interface xgigabitethernet 0/0/2
[CE2-XGigabitEthernet0/0/2] port link-type trunk
[CE2-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[CE2-XGigabitEthernet0/0/2] stp disable
[CE2-XGigabitEthernet0/0/2] quit
```

- Configure UPE A.

  # Disable STP on the interfaces that need to be added to the RRPP ring on UPE A. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEA] interface xgigabitethernet 0/0/1
[UPEA-XGigabitEthernet0/0/1] port link-type trunk
[UPEA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-XGigabitEthernet0/0/1] stp disable
[UPEA-XGigabitEthernet0/0/1] quit
[UPEA] interface xgigabitethernet 0/0/2
[UPEA-XGigabitEthernet0/0/2] port link-type trunk
[UPEA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-XGigabitEthernet0/0/2] stp disable
[UPEA-XGigabitEthernet0/0/2] quit
```

- # Configure UPE B.

  # Disable STP on the interfaces that need to be added to the RRPP ring on UPE B. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEB] interface xgigabitethernet 0/0/1
[UPEB-XGigabitEthernet0/0/1] port link-type trunk
[UPEB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-XGigabitEthernet0/0/1] stp disable
[UPEB-XGigabitEthernet0/0/1] quit
[UPEB] interface xgigabitethernet 0/0/2
[UPEB-XGigabitEthernet0/0/2] port link-type trunk
[UPEB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-XGigabitEthernet0/0/2] stp disable
[UPEB-XGigabitEthernet0/0/2] quit
[UPEB] interface xgigabitethernet 0/0/3
[UPEB-XGigabitEthernet0/0/3] port link-type trunk
[UPEB-XGigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPEB-XGigabitEthernet0/0/3] stp disable
[UPEB-XGigabitEthernet0/0/3] quit
[UPEB] interface xgigabitethernet 0/0/4
[UPEB-XGigabitEthernet0/0/4] port link-type trunk
[UPEB-XGigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPEB-XGigabitEthernet0/0/4] stp disable
[UPEB-XGigabitEthernet0/0/4] quit
```

- Configure UPE C.

  # Disable STP on the interfaces that need to be added to the RRPP ring on UPE C. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEC] interface xgigabitethernet 0/0/1
[UPEC-XGigabitEthernet0/0/1] port link-type trunk
[UPEC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/1] stp disable
[UPEC-XGigabitEthernet0/0/1] quit
[UPEC] interface xgigabitethernet 0/0/2
[UPEC-XGigabitEthernet0/0/2] port link-type trunk
```

```
[UPEC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/2] stp disable
[UPEC-XGigabitEthernet0/0/2] quit
[UPEC] interface xgigabitethernet 0/0/3
[UPEC-XGigabitEthernet0/0/3] port link-type trunk
[UPEC-XGigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/3] stp disable
[UPEC-XGigabitEthernet0/0/3] quit
[UPEC] interface xgigabitethernet 0/0/4
[UPEC-XGigabitEthernet0/0/4] port link-type trunk
[UPEC-XGigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/4] stp disable
[UPEC-XGigabitEthernet0/0/4] quit
```

- Configure UPE D.

  # Disable STP on the interfaces that need to be added to the RRPP ring on UPE D. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPED] interface xgigabitethernet 0/0/1
[UPED-XGigabitEthernet0/0/1] port link-type trunk
[UPED-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPED-XGigabitEthernet0/0/1] stp disable
[UPED-XGigabitEthernet0/0/1] quit
[UPED] interface xgigabitethernet 0/0/2
[UPED-XGigabitEthernet0/0/2] port link-type trunk
[UPED-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPED-XGigabitEthernet0/0/2] stp disable
[UPED-XGigabitEthernet0/0/2] quit
```

- Configure PE-AGG.

  # Disable STP of the interfaces that need to be added to the RRPP ring on PE-AGG. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[PE-AGG] interface xgigabitethernet 0/0/1
[PE-AGG-XGigabitEthernet0/0/1] port link-type trunk
[PE-AGG-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-XGigabitEthernet0/0/1] stp disable
[PE-AGG-XGigabitEthernet0/0/1] quit
[PE-AGG] interface xgigabitethernet 0/0/2
[PE-AGG-XGigabitEthernet0/0/2] port link-type trunk
[PE-AGG-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-XGigabitEthernet0/0/2] stp disable
[PE-AGG-XGigabitEthernet0/0/2] quit
```

Step 3 Create RRPP domains and configure the protected VLANs and control VLANs.

- Configure CE1.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[CE1] rrpp domain 1
[CE1-rrpp-domain-region1] protected-vlan reference-instance 1
[CE1-rrpp-domain-region1] control-vlan 5
[CE1-rrpp-domain-region1] quit
```

  # Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[CE1] rrpp domain 2
[CE1-rrpp-domain-region2] protected-vlan reference-instance 2
[CE1-rrpp-domain-region2] control-vlan 10
[CE1-rrpp-domain-region2] quit
```

- Configure CE2.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[CE2] rrpp domain 1
[CE2-rrpp-domain-region1] protected-vlan reference-instance 1
```

```
[CE2-rrpp-domain-region1] control-vlan 5
[CE2-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[CE2] rrpp domain 2
[CE2-rrpp-domain-region2] protected-vlan reference-instance 2
[CE2-rrpp-domain-region2] control-vlan 10
[CE2-rrpp-domain-region2] quit
```

- Configure UPE A.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

  ```
  [UPEA] rrpp domain 1
  [UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
  [UPEA-rrpp-domain-region1] control-vlan 5
  [UPEA-rrpp-domain-region1] quit
  ```

  # Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

  ```
  [UPEA] rrpp domain 2
  [UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
  [UPEA-rrpp-domain-region2] control-vlan 10
  [UPEA-rrpp-domain-region2] quit
  ```

- # Configure UPE B.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

  ```
  [UPEB] rrpp domain 1
  [UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
  [UPEB-rrpp-domain-region1] control-vlan 5
  [UPEB-rrpp-domain-region1] quit
  ```

  # Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

  ```
  [UPEB] rrpp domain 2
  [UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
  [UPEB-rrpp-domain-region2] control-vlan 10
  [UPEB-rrpp-domain-region2] quit
  ```

- Configure UPE C.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

  ```
  [UPEC] rrpp domain 1
  [UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
  [UPEC-rrpp-domain-region1] control-vlan 5
  [UPEC-rrpp-domain-region1] quit
  ```

  # Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

  ```
  [UPEC] rrpp domain 2
  [UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
  [UPEC-rrpp-domain-region2] control-vlan 10
  [UPEC-rrpp-domain-region2] quit
  ```

- Configure UPE D.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

  ```
  [UPED] rrpp domain 1
  [UPED-rrpp-domain-region1] protected-vlan reference-instance 1
  [UPED-rrpp-domain-region1] control-vlan 5
  [UPED-rrpp-domain-region1] quit
  ```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] protected-vlan reference-instance 2
[UPED-rrpp-domain-region2] control-vlan 10
[UPED-rrpp-domain-region2] quit
```

- Configure PE-AGG.

  # Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 5
[PE-AGG-rrpp-domain-region1] quit
```

  # Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] protected-vlan reference-instance 2
[PE-AGG-rrpp-domain-region2] control-vlan 10
[PE-AGG-rrpp-domain-region2] quit
```

Step 4 Create an RRPP ring.

- Configure PE-AGG.

  # Configure PE-AGG as the master node of ring 1 in domain 1. Configure XGE 0/0/1 as the primary port and XGE 0/0/2 as the secondary port.

```
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

  # Configure PE-AGG as the master node of ring 1 in domain 2. Configure XGE 0/0/2 as the primary port and XGE 0/0/1 as the secondary port.

```
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] ring 1 node-mode master primary-port
xgigabitethernet 0/0/2 secondary-port xgigabitethernet 0/0/1 level 0
[PE-AGG-rrpp-domain-region2] ring 1 enable
[PE-AGG-rrpp-domain-region2] quit
```

- Configure UPE A.

  # Configure UPE A as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE A.

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

  # Configure UPE A as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE A.

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- Configure UPE D.

  # Configure UPE D as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE D.

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] ring 1 node-mode transit primary-port
```

```
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPED-rrpp-domain-region1] ring 1 enable
[UPED-rrpp-domain-region1] quit
```

Configure UPE D as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE D.

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPED-rrpp-domain-region2] ring 1 enable
[UPED-rrpp-domain-region2] quit
```

- # Configure UPE B.

  # Configure UPE B as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE B.

  ```
  [UPEB] rrpp domain 1
  [UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port
  xgigabitethernet 0/0/1 secondary-port gxgigabitethernet 0/0/2 level 0
  [UPEB-rrpp-domain-region1] ring 1 enable
  [UPEB-rrpp-domain-region1] quit
  ```

  # Configure UPE B as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE B.

  ```
  [UPEB] rrpp domain 2
  [UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port
  xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
  [UPEB-rrpp-domain-region2] ring 1 enable
  [UPEB-rrpp-domain-region2] quit
  ```

  # Configure UPE B as an edge node of ring 2 in domain 1. Configure XGE 0/0/1 as the public port and XGE 0/0/3 as the edge port.

  ```
  [UPEB] rrpp domain 1
  [UPEB-rrpp-domain-region1] ring 2 node-mode edge common-port xgigabitethernet
  0/0/1 edge-port xgigabitethernet 0/0/3
  [UPEB-rrpp-domain-region1] ring 2 enable
  [UPEB-rrpp-domain-region1] quit
  ```

  # Configure UPE B as an edge node of ring 2 in domain 2. Configure XGE 0/0/1 as the public port and XGE 0/0/3 as the edge port.

  ```
  [UPEB] rrpp domain 2
  [UPEB-rrpp-domain-region2] ring 2 node-mode edge common-port xgigabitethernet
  0/0/1 edge-port xgigabitethernet 0/0/3
  [UPEB-rrpp-domain-region2] ring 2 enable
  [UPEB-rrpp-domain-region2] quit
  ```

  # Configure UPE B as an edge node of ring 3 in domain 1. Configure XGE 0/0/1 as the public port and XGE 0/0/4 as the edge port.

  ```
  [UPEB] rrpp domain 1
  [UPEB-rrpp-domain-region1] ring 3 node-mode edge common-port xgigabitethernet
  0/0/1 edge-port xgigabitethernet 0/0/4
  [UPEB-rrpp-domain-region1] ring 3 enable
  [UPEB-rrpp-domain-region1] quit
  ```

  # Configure UPE B as an edge node of ring 3 in domain 2. Configure XGE 0/0/1 as the public port and XGE 0/0/4 as the edge port.

  ```
  [UPEB] rrpp domain 2
  [UPEB-rrpp-domain-region2] ring 3 node-mode edge common-port xgigabitethernet
  0/0/1 edge-port xgigabitethernet 0/0/4
  [UPEB-rrpp-domain-region2] ring 3 enable
  [UPEB-rrpp-domain-region2] quit
  ```

- Configure UPE C.

  # Configure UPE C as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE C.

  ```
  [UPEC] rrpp domain 1
  [UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port
  ```

```
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

Configure UPE C as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE C.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port
xgigabitethernet 0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

Configure UPE B as an edge node of ring 2 in domain 1. Configure XGE 0/0/2 as the public port and XGE 0/0/3 as the edge port.

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 2 node-mode assistant-edge common-port
xgigabitethernet 0/0/2 edge-port xgigabitethernet 0/0/3
[UPEC-rrpp-domain-region1] ring 2 enable
[UPEC-rrpp-domain-region1] quit
```

Configure UPE B as an edge node of ring 2 in domain 2. Configure XGE 0/0/2 as the public port and XGE 0/0/3 as the edge port.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 2 node-mode assistant-edge common-port
xgigabitethernet 0/0/2 edge-port xgigabitethernet 0/0/3
[UPEC-rrpp-domain-region2] ring 2 enable
[UPEC-rrpp-domain-region2] quit
```

Configure UPE C as an edge node of ring 3 in domain 1. Configure XGE 0/0/1 as the public port and XGE 0/0/4 as the edge port.

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 3 node-mode assistant-edge common-port
xgigabitethernet 0/0/2 edge-port xgigabitethernet 0/0/4
[UPEC-rrpp-domain-region1] ring 3 enable
[UPEC-rrpp-domain-region1] quit
```

Configure UPE C as an edge node of ring 3 in domain 2. Configure XGE 0/0/2 as the public port and XGE 0/0/4 as the edge port.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 3 node-mode assistant-edge common-port
xgigabitethernet 0/0/2 edge-port xgigabitethernet 0/0/4
[UPEC-rrpp-domain-region2] ring 3 enable
[UPEC-rrpp-domain-region2] quit
```

- Configure CE1.

  # Configure CE1 as the master node of ring 2 in domain 1. Configure XGE 0/0/1 as the primary port and XGE 0/0/2 as the secondary port.

  ```
  [CE1] rrpp domain 1
  [CE1-rrpp-domain-region1] ring 2 node-mode master primary-port xgigabitethernet
  0/0/1 secondary-port xgigabitethernet 0/0/2 level 1
  [CE1-rrpp-domain-region1] ring 2 enable
  [CE1-rrpp-domain-region1] quit
  ```

  # Configure CE1 as the master node of ring 2 in domain 2. Configure XGE 0/0/2 as the primary port and XGE 0/0/1 as the secondary port.

  ```
  [CE1] rrpp domain 2
  [CE1-rrpp-domain-region2] ring 2 node-mode master primary-port xgigabitethernet
  0/0/2 secondary-port xgigabitethernet 0/0/1 level 1
  [CE1-rrpp-domain-region2] ring 2 enable
  [CE1-rrpp-domain-region2] quit
  ```

- Configure CE2.

  # Configure CE2 as the master node of ring 3 in domain 1. Configure XGE 0/0/1 as the primary port and XGE 0/0/2 as the secondary port.

  ```
  [CE2] rrpp domain 1
  [CE2-rrpp-domain-region1] ring 3 node-mode master primary-port xgigabitethernet
  ```

```
0/0/1 secondary-port xgigabitethernet 0/0/2 level 1
[CE2-rrpp-domain-region1] ring 3 enable
[CE2-rrpp-domain-region1] quit
```

Configure CE2 as the master node of ring 3 in domain 2. Configure XGE 0/0/2 as the primary port and XGE 0/0/1 as the secondary port.

```
[CE2] rrpp domain 2
[CE2-rrpp-domain-region2] ring 3 node-mode master primary-port xgigabitethernet
0/0/2 secondary-port xgigabitethernet 0/0/1 level 1
[CE2-rrpp-domain-region2] ring 3 enable
[CE2-rrpp-domain-region2] quit
```

Step 5 Enable the RRPP protocol.

After configuring an RRPP ring, you need to enable RRPP on each node on the ring to activate the RRPP ring. The configuration procedure is as follows:

- Configure PE-AGG.

  # Enable the RRPP protocol.

  ```
  [PE-AGG] rrpp enable
  ```

- Configure UPE A.

  # Enable the RRPP protocol.

  ```
  [UPEA] rrpp enable
  ```

- Configure UPE D.

  # Enable the RRPP protocol.

  ```
  [UPED] rrpp enable
  ```

- # Configure UPE B.

  # Enable the RRPP protocol.

  ```
  [UPEB] rrpp enable
  ```

- Configure UPE C.

  # Enable the RRPP protocol.

  ```
  [UPEC] rrpp enable
  ```

- Configure CE1.

  # Enable the RRPP protocol.

  ```
  [CE1] rrpp enable
  ```

- Configure CE2.

  # Enable the RRPP protocol.

  ```
  [CE2] rrpp enable
  ```

Step 6 Configure a ring group.

- Configure UPE C (assistant edge node).

  # Create ring group 1, which consists of four subrings: ring 2 in domain 1, ring 3 in domain 1, ring 2 in domain 2, and ring 3 in domain 2.

  ```
  [UPEC] rrpp ring-group 1
  [UPEC-rrpp-ring-group1] domain 1 ring 2 to 3
  [UPEC-rrpp-ring-group1] domain 2 ring 2 to 3
  [UPEC-rrpp-ring-group1] quit
  ```

- Configure UPE B (edge node).

  # Create ring group 1, which consists of four subrings: ring 2 in domain 1, ring 3 in domain 1, ring 2 in domain 2, and ring 3 in domain 2.

  ```
  [UPEB] rrpp ring-group 1
  [UPEB-rrpp-ring-group1] domain 1 ring 2 to 3
  ```

```
[UPEB-rrpp-ring-group1] domain 2 ring 2 to 3
[UPEB-rrpp-ring-group1] quit
```

Step 7 Set the link-Up timer.

- Configure CE1.

  # Set the link-Up timer to 1 second.

  ```
  [CE1] rrpp linkup-delay-timer 1
  ```

- Configure CE2.

  # Set the link-Up timer to 1 second.

  ```
  [CE2] rrpp linkup-delay-timer 1
  ```

- Configure PE-AGG.

  # Set the link-Up timer to 1 second.

  ```
  [PE-AGG] rrpp linkup-delay-timer 1
  ```

Step 8 Verify the configuration.

After the preceding configurations are complete and the network topology becomes stable, perform the following operations to verify the configuration. Here, UPE B and PE-AGG are used as examples.

- Run the **display rrpp brief** command on UPE B. The following information is displayed.

```
[UPEB] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common         Secondary/Edge           Is
 ID     Level   Mode     Port                   Port
Enabled

------------------------------------------------------------------------------
--
 1      0       T        XGigabitEthernet0/0/1   XGigabitEthernet0/0/2     Yes
 2      1       E        XGigabitEthernet0/0/1   XGigabitEthernet0/0/3     Yes
 3      1       E        XGigabitEthernet0/0/1   XGigabitEthernet0/0/4     Yes

Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge           Is
 ID     Level   Mode     Port                    Port
Enabled

------------------------------------------------------------------------------
--
 1      0        T       XGigabitEthernet0/0/1    XGigabitEthernet0/0/2    Yes
 2      1        E       XGigabitEthernet0/0/1    XGigabitEthernet0/0/3    Yes
 3      1        E       XGigabitEthernet0/0/1    XGigabitEthernet0/0/4    Yes
```

You can see that the RRPP protocol is enabled on UPE B.

In domain 1:

VLAN 5 is the control VLAN and VLANs mapping instance 1 are the protected VLANs.

UPE B is a transit node on ring 1; XGE 0/0/1 is the primary port; XGE 0/0/2 is the secondary port.

UPE B is an edge transit node on ring 2. XGE 0/0/1 is the public port and XGE 0/0/3 is the edge port.

UPE B is an edge transit node on ring 3. XGE 0/0/1 is the public port and XGE 0/0/4 is the edge port.

In domain 2:

VLAN 10 is the control VLAN and VLANs mapping instance 2 are the protected VLANs.

UPE B is a transit node on ring 1. XGE 0/0/1 is the primary port, and XGE 0/0/2 is the secondary port.

UPE B is an edge transit node on ring 2. XGE 0/0/1 is the public port and XGE 0/0/3 is the edge port.

UPE B is an edge transit node on ring 3. XGE 0/0/1 is the public port and XGE 0/0/4 is the edge port.

- Run the **display rrpp brief** command on PE-AGG. The following information is displayed:

```
[PE-AGG] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status:  Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common          Secondary/Edge          Is
 ID     Level   Mode     Port                    Port
Enabled

------------------------------------------------------------------------------
--
 1      0       M        XGigabitEthernet0/0/1    XGigabitEthernet0/0/2     Yes

Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring   Ring    Node     Primary/Common           Secondary/Edge          Is
 ID     Level   Mode     Port                     Port
Enabled

------------------------------------------------------------------------------
--
 1      0       M        XGigabitEthernet0/0/2     XGigabitEthernet0/0/1    Yes
```

The preceding information shows that the RRPP protocol is enabled on PE-AGG, and the link-Up timer is 2 seconds.

In domain 1, VLAN 5 is the control VLAN; VLANs mapping instance 1 are the protected VLANs; PE-AGG is the master node on ring 1. XGE 0/0/1 is the primary port, and XGE 0/0/2 is the secondary port.

In domain 2, VLAN 10 is the control VLAN; VLANs mapping instance 2 are the protected VLANs; PE-AGG is the master node on ring 1. XGE 0/0/2 is the primary port, and XGE 0/0/1 is the secondary port.

- Run the **display rrpp verbose domain** command on UPE B. You can obtain the following results:

View detailed information about UPE B in domain 1.

```
[UPEB] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                              Is Active : Yes
Primary port  :  XGigabitEthernet0/0/1         Port status: UP
Secondary port:  XGigabitEthernet0/0/2         Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                               Is Active : Yes
Common port   :  XGigabitEthernet0/0/1         Port status: UP
Edge port     :  XGigabitEthernet0/0/3         Port status: UP

RRPP Ring     : 3
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                              Is Active : Yes
Common port   :  XGigabitEthernet0/0/1         Port status: UP
Edge port     :  XGigabitEthernet0/0/4         Port status: UP
```

The preceding information shows that VLAN 5 is the control VLAN in domain 1, and VLANs mapping instance 1 are the protected VLANs.

UPE B is a transit node on ring 1 in domain 1 and is in LinkUp state.

UPE B is a transit node on ring 2 in domain 1 and is in LinkUp state. XGE 0/0/1 is the public port, and XGE 0/0/3 is the edge port.

UPE B is a transit node on ring 3 in domain 1 and is in LinkUp state. XGE 0/0/1 is the public port, and XGE 0/0/4 is the edge port.

View detailed information about UPE B in domain 2.

```
[UPEB] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : LinkUp
Is Enabled    : Enable                              Is Active : Yes
Primary port  :  XGigabitEthernet0/0/1         Port status: UP
Secondary port:  XGigabitEthernet0/0/2         Port status: UP

RRPP Ring     : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
Is Enabled    : Enable                              Is Active : Yes
Common port   :  XGigabitEthernet0/0/1         Port status: UP
Edge port     :  XGigabitEthernet0/0/3         Port status: UP

RRPP Ring     : 3
Ring Level    : 1
Node Mode     : Edge
Ring State    : LinkUp
```

```
Is Enabled    : Enable                              Is Active : Yes
Common port   :  XGigabitEthernet0/0/1         Port status: UP
Edge port     :  XGigabitEthernet0/0/4         Port status: UP
```

The preceding information shows that VLAN 10 is the control VLAN in domain 2, and VLANs mapping instance 2 are the protected VLANs.

UPE B is a transit node in domain 2 and is in LinkUp state.

UPE B is a transit node on ring 2 in domain 2 and is in LinkUp state. XGE 0/0/1 is the public port, and XGE 0/0/3 is the edge port.

UPE B is a transit node on ring 3 in domain 2 and is in LinkUp state. XGE 0/0/1 is the public port, and XGE 0/0/4 is the edge port.

- Run the **display rrpp verbose domain** command on PE-AGG. You can obtain the following results:

  # View detailed information about PE-AGG in domain 1.

```
[PE-AGG] display rrpp verbose domain 1
Domain Index  : 1
Control VLAN  : major 5    sub 6
Protected VLAN: Reference Instance 1
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                              Is Active : Yes
Primary port  :  XGigabitEthernet0/0/1         Port status: UP
Secondary port:  XGigabitEthernet0/0/2         Port status: BLOCKED
```

  The preceding information shows that VLAN 5 is the control VLAN in domain 1, and VLANs mapping instance 1 are the protected VLANs.

  PE-AGG is the master node in domain 1 and is in Complete state.

  XGE 0/0/1 is the primary port, and XGE 0/0/2 is the secondary port.

  # View detailed information about PE-AGG in domain 2.

```
[PE-AGG] display rrpp verbose domain 2
Domain Index  : 2
Control VLAN  : major 10    sub 11
Protected VLAN: Reference Instance 2
Hello Timer   : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Is Enabled    : Enable                              Is Active : Yes
Primary port  :  XGigabitEthernet0/0/2         Port status: UP
Secondary port:  XGigabitEthernet0/0/1         Port status: BLOCKED
```

  The preceding information shows that VLAN 10 is the control VLAN in domain 2, and VLANs mapping instance 2 are the protected VLANs.

  PE-AGG is the master node in domain 2 and is in Complete state.

  XGE 0/0/2 is the primary port, and XGE 0/0/1 is the secondary port.

- Run the **display rrpp ring-group** command on UPE B to view the configuration of the ring group.

  # View the configuration of ring group 1.

```
[UPEB] display rrpp ring-group 1
 Ring Group 1:
```

```
domain 1 ring 2 to 3
domain 2 ring 2 to 3
```

----End

Configuration Files

- Configuration file of CE1

```
#
sysname CE1
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 1
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 1
 ring 2 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 2 node-mode master primary-port XGigabitEthernet 0/0/2 secondary-port
XGigabitEthernet 0/0/1 level 1
 ring 2 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- Configuration file of CE2

```
#
#
sysname CE2
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 1
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 3 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 1
 ring 3 enable
rrpp domain 2
```

```
 control-vlan 10
 protected-vlan reference-instance 2
 ring 3 node-mode master primary-port XGigabitEthernet 0/0/2 secondary-port
XGigabitEthernet 0/0/1 level 1
 ring 3 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE A

```
#
#
sysname UPEA
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE B

```
#
sysname UPEB
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
```

```
rrpp domain 1
control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge common-port XGigabitEthernet 0/0/1 edge-port
XGigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode edge common-port XGigabitEthernet 0/0/1 edge-port
XGigabitEthernet 0/0/4
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge common-port XGigabitEthernet 0/0/1 edge-port
XGigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode edge common-port XGigabitEthernet 0/0/1 edge-port
XGigabitEthernet 0/0/4
 ring 3 enable
#
rrpp ring-group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE C

```
#
sysname UPEC
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
```

```
 ring 2 node-mode assistant-edge common-port XGigabitEthernet 0/0/2 edge-
portXGigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge common-port XGigabitEthernet 0/0/2 edge-port
XGigabitEthernet 0/0/4
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-
portXGigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port XGigabitEthernet 0/0/2 edge-port
XGigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge common-port XGigabitEthernet 0/0/2 edge-port
XGigabitEthernet 0/0/4
 ring 3 enable
#
rrpp ring-group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan  6 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 6 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE D

```
#
sysname UPED
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
```

```
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of PE-AGG

```
#
sysname PE-AGG
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 1
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/2 secondary-port
XGigabitEthernet 0/0/1 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

7.3.6 Example for Configuring Tangent RRPP Rings with Multiple Instances

Networking Requirements

As shown in **Figure 7-10**, UPE A, UPE B, UPE C, and UPE D form two multi-instance rings: ring 1 in domain 1 and ring 1 in domain 2. UPE D, UPE E, UPE F, and UPE G form ring 1 in domain 3. Packets of the data VLANs connected to CE are forwarded to the backbone network through the two tangent rings.

The tangent point of the two rings is UPE D.

VLANs 100 to 300 are configured on CE. Domain 1 and domain 2 share the traffic of packets from VLANs 100 to 300. Packets from VLANs 100 to 200 are transmitted through domain 1, and packets from VLANs 201 to 300 are transmitted through domain 2.

Table 7-6 shows the mapping between protected VLANs and instances in domain 1, domain 2, and domain 3.

Table 7-6 Mapping between protected VLANs and instances

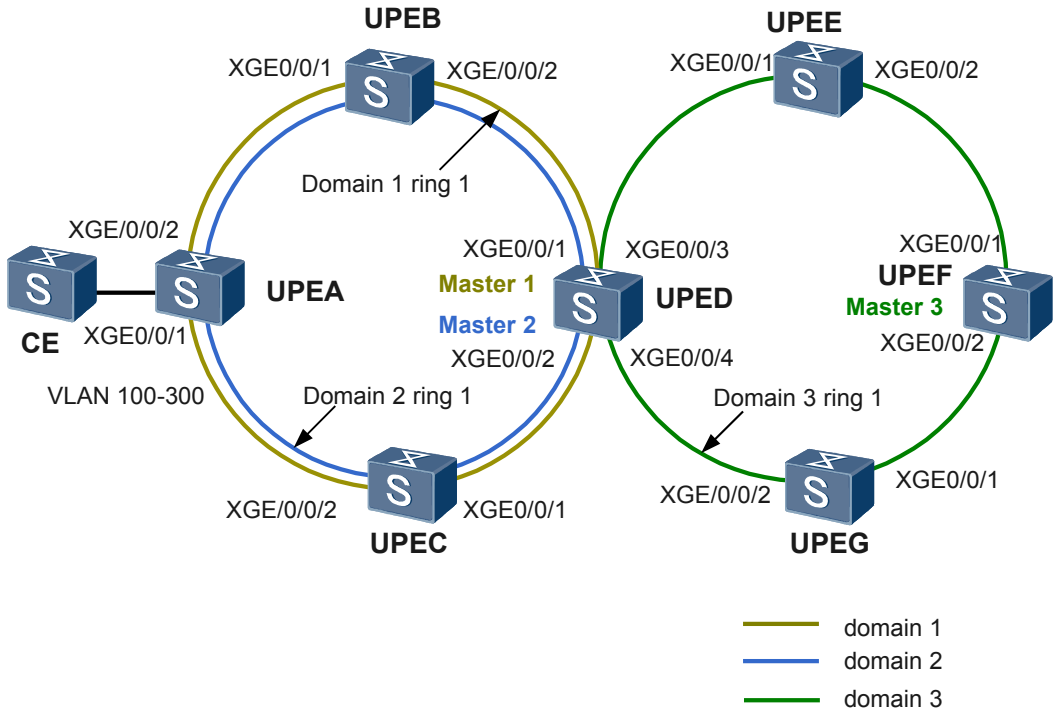
Domain ID	Control VLAN	Instance ID	Protected VLAN	Instance ID
Domain 1	VLAN 5, 6	Instance 1	VLAN 100-200	Instance 1
Domain 2	VLAN 10, 11	Instance 2	VLAN 201-300	Instance 2
Domain 3 (on UPE D)	VLAN 20, 21	Instance 3	VLAN 100-300	Instance 1 and instance 2
Domain 3	VLAN 20, 21	Instance 1	VLAN 100-300	Instance 1

Table 7-7 shows the master node of each ring, and the primary port and secondary port on each master node.

Table 7-7 Master nodes, and primary and secondary ports on the master nodes

Ring ID	Master Node	Primary Port	Secondary Port
Ring 1 in domain 1	UPE D	XGE 0/0/1	XGE 0/0/2
Ring 1 in domain 2	UPE D	XGE 0/0/2	XGE 0/0/1
Ring 1 in domain 3	UPE F	XGE 0/0/1	XGE 0/0/2

Figure 7-10 Networking diagram of tangent RRPP rings with multiple instances



Configuration Roadmap

The configuration roadmap is as follows:

1. Map instance 1 to VLANs 100 to 200. Map instance 2 to VLANs 201 to 300.
2. Add UPE A, UPE B, UPE C, and UPE D to ring 1 in domain 1 and ring 1 in domain 2.
3. Add UPE D, UPE E, UPE F, and UPE G to ring 1 in domain 3.
4. Configure protected VLANs in domain 1 and domain 2.
5. Configure control VLANs in domain 1 and domain 2.
6. Configure the control VLAN in domain 3.
7. Configure UPE D as the master node and configure UPE A, UPE B, and UPE C as transit nodes on ring 1 in domain 1 and ring 1 in domain 2.
8. Configure UPE F as the master node and configure UPE D, UPE E, and UPE G as transit nodes on ring 1 in domain 3.

Data Preparation

To complete the configuration, you need the following data:

- Instance IDs
- Range of the protected VLANs
- IDs of the control VLANs
- Numbers of the RRPP interfaces

Procedure

Step 1 Create instances.

- Configure UPE A.

Create data VLANs 100 to 300 on UPE A.

```
<Quidway> system-view
[Quidway] sysname UPEA
[UPEA] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPEA-mst-region] active region-configuration
[UPEA-mst-region] quit
```

- # Configure UPE B.

Create data VLANs 100 to 300 on UPE B.

```
<Quidway> system-view
[Quidway] sysname UPEB
[UPEB] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPEB-mst-region] active region-configuration
[UPEB-mst-region] quit
```

- Configure UPE C.

Create data VLANs 100 to 300 on UPE C.

```
<Quidway> system-view
[Quidway] sysname UPEC
[UPEC] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[UPEC-mst-region] active region-configuration
[UPEC-mst-region] quit
```

- Configure UPE D.

Create data VLANs 100 to 300 on UPE D.

```
<Quidway> system-view
[Quidway] sysname UPED
[UPED] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 5 and VLAN 6 and data VLANs 100 to 200 in domain 1.

```
[UPED] stp region-configuration
[UPED-mst-region] instance 1 vlan 5 6 100 to 200
```

Create instance 2 and map it to control VLANs VLAN 10 and VLAN 11 and data VLANs 201 to 300 in domain 2.

```
[UPED-mst-region] instance 2 vlan 10 11 201 to 300
```

Create instance 3 and map it to control VLANs VLAN 20 and VLAN 21 in domain 3.

```
[UPED-mst-region] instance 3 vlan 20 21
```

Activate the configuration.

```
[UPED-mst-region] active region-configuration
[UPED-mst-region] quit
```

- Configure UPE E.

Create data VLANs 100 to 300 on UPE E.

```
<Quidway> system-view
[Quidway] sysname UPEE
[UPEE] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 20 and VLAN 21 and data VLANs 100 to 300 in domain 3.

```
[UPEE] stp region-configuration
[UPEE-mst-region] instance 1 vlan 20 21 100 to 300
```

Activate the configuration.

```
[UPEE-mst-region]  active region-configuration
[UPEE-mst-region] quit
```

- Configure UPE F.

Create data VLANs 100 to 300 on UPE F.

```
<Quidway> system-view
[Quidway] sysname UPEF
[UPEF] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 20 and VLAN 21 and data VLANs 100 to 300 in domain 3.

```
[UPEF] stp region-configuration
[UPEF-mst-region] instance 1 vlan 20 21 100 to 300
```

Activate the configuration.

```
[UPEF-mst-region] active region-configuration
[UPEF-mst-region] quit
```

- Configure UPE G.

Create data VLANs 100 to 300 on UPE G.

```
<Quidway> system-view
[Quidway] sysname UPEG
[UPEG] vlan batch 100 to 300
```

Create instance 1 and map it to control VLANs VLAN 20 and VLAN 21 and data VLANs 100 to 300 in domain 3.

```
[UPEG] stp region-configuration
[UPEG-mst-region] instance 1 vlan 20 21 100 to 300
```

Activate the configuration.

```
[UPEG-mst-region] active region-configuration
[UPEG-mst-region] quit
```

- Verify the configuration.

Run the **display stp region-configuration** command on the devices to view the mapping between instances and VLANs. The displayed information on UPE A is as follows:

```
[UPEA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e0cd568d00
   Revision level     :0

Instance   Vlans Mapped
   0       1 to 4, 7 to 9, 12 to 99, 301 to 4094
   1       5 to 6, 100 to 200
   2       10 to 11, 201 to 300
```

Step 2 Configure RRPP interfaces.

- Configure UPE A.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE A. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEA] interface xgigabitethernet 0/0/1
[UPEA-XGigabitEthernet0/0/1] port link-type trunk
[UPEA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-XGigabitEthernet0/0/1] stp disable
[UPEA-XGigabitEthernet0/0/1] quit
[UPEA] interface xgigabitethernet 0/0/2
[UPEA-XGigabitEthernet0/0/2] port link-type trunk
[UPEA-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-XGigabitEthernet0/0/2] stp disable
[UPEA-XGigabitEthernet0/0/2] quit
```

- # Configure UPE B.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE B. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEB] interface xgigabitethernet 0/0/1
[UPEB-XGigabitEthernet0/0/1] port link-type trunk
[UPEB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-XGigabitEthernet0/0/1] stp disable
[UPEB-XGigabitEthernet0/0/1] quit
[UPEB] interface xgigabitethernet 0/0/2
[UPEB-XGigabitEthernet0/0/2] port link-type trunk
[UPEB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
```

```
[UPEB-XGigabitEthernet0/0/2] stp disable
[UPEB-XGigabitEthernet0/0/2] quit
```

- Configure UPE C.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE C. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEC] interface xgigabitethernet 0/0/1
[UPEC-XGigabitEthernet0/0/1] port link-type trunk
[UPEC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/1] stp disable
[UPEC-XGigabitEthernet0/0/1] quit
[UPEC] interface xgigabitethernet 0/0/2
[UPEC-XGigabitEthernet0/0/2] port link-type trunk
[UPEC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-XGigabitEthernet0/0/2] stp disable
[UPEC-XGigabitEthernet0/0/2] quit
```

- Configure UPE D.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE D. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPED] interface xgigabitethernet 0/0/1
[UPED-XGigabitEthernet0/0/1] port link-type trunk
[UPED-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPED-XGigabitEthernet0/0/1] stp disable
[UPED-XGigabitEthernet0/0/1] quit
[UPED] interface xgigabitethernet 0/0/3
[UPED-XGigabitEthernet0/0/3] port link-type trunk
[UPED-XGigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPED-XGigabitEthernet0/0/3] stp disable
[UPED-XGigabitEthernet0/0/3] quit
[UPED] interface xgigabitethernet 0/0/2
[UPED-XGigabitEthernet0/0/2] port link-type trunk
[UPED-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPED-XGigabitEthernet0/0/2] stp disable
[UPED-XGigabitEthernet0/0/2] quit
[UPED] interface xgigabitethernet 0/0/4
[UPED-XGigabitEthernet0/0/4] port link-type trunk
[UPED-XGigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPED-XGigabitEthernet0/0/4] stp disable
[UPED-XGigabitEthernet0/0/4] quit
```

- Configure UPE E.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE E. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEE] interface xgigabitethernet 0/0/1
[UPEE-XGigabitEthernet0/0/1] port link-type trunk
[UPEE-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEE-XGigabitEthernet0/0/1] stp disable
[UPEE-XGigabitEthernet0/0/1] quit
[UPEE] interface xgigabitethernet 0/0/2
[UPEE-XGigabitEthernet0/0/2] port link-type trunk
[UPEE-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEE-XGigabitEthernet0/0/2] stp disable
[UPEE-XGigabitEthernet0/0/2] quit
```

- Configure UPE F.

Disable STP on the interfaces that need to be added to the RRPP ring on UPE F. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEF] interface xgigabitethernet 0/0/1
[UPEF-XGigabitEthernet0/0/1] port link-type trunk
[UPEF-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEF-XGigabitEthernet0/0/1] stp disable
```

```
[UPEF-XGigabitEthernet0/0/1] quit
[UPEF] interface xgigabitethernet 0/0/2
[UPEF-XGigabitEthernet0/0/2] port link-type trunk
[UPEF-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEF-XGigabitEthernet0/0/2] stp disable
[UPEF-XGigabitEthernet0/0/2] quit
```

- Configure UPE G.

Disable the STP function on the interfaces to be added to the RRPP ring on UPE G. Configure the RRPP interfaces to allow packets of VLANs 100 to 300 to pass through.

```
[UPEG] interface xgigabitethernet 0/0/1
[UPEG-XGigabitEthernet0/0/1] port link-type trunk
[UPEG-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEG-XGigabitEthernet0/0/1] stp disable
[UPEG-XGigabitEthernet0/0/1] quit
[UPEG] interface xgigabitethernet 0/0/2
[UPEG-XGigabitEthernet0/0/2] port link-type trunk
[UPEG-XGigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEG-XGigabitEthernet0/0/2] stp disable
[UPEG-XGigabitEthernet0/0/2] quit
```

Step 3 Create RRPP domains and configure the protected VLANs and control VLANs.

- Configure UPE A.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 5
[UPEA-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- # Configure UPE B.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 5
[UPEB-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 5
[UPEC-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- Configure UPE D.

Configure the VLANs mapping instance 1 as the protected VLANs in domain 1. Configure VLAN 5 as the control VLAN.

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] protected-vlan reference-instance 1
[UPED-rrpp-domain-region1] control-vlan 5
[UPED-rrpp-domain-region1] quit
```

Configure the VLANs mapping instance 2 as the protected VLANs in domain 2. Configure VLAN 10 as the control VLAN.

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] protected-vlan reference-instance 2
[UPED-rrpp-domain-region2] control-vlan 10
[UPED-rrpp-domain-region2] quit
```

Configure the VLANs mapping instances 1 to 3 as the protected VLANs in domain 3. Configure VLAN 20 as the control VLAN.

```
[UPED] rrpp domain 3
[UPED-rrpp-domain-region3] protected-vlan reference-instance 1 2 3
[UPED-rrpp-domain-region3] control-vlan 20
[UPED-rrpp-domain-region3] quit
```

- Configure UPE E.

Configure VLAN 20 as the control VLAN in domain 3.

```
[UPEE] rrpp domain 3
[UPEE-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEE-rrpp-domain-region3] control-vlan 20
[UPEE-rrpp-domain-region3] quit
```

- Configure UPE F.

Configure VLAN 20 as the control VLAN in domain 3.

```
[UPEF] rrpp domain 3
[UPEF-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEF-rrpp-domain-region3] control-vlan 20
[UPEF-rrpp-domain-region3] quit
```

- Configure UPE G.

Configure VLAN 20 as the control VLAN in domain 3.

```
[UPEG] rrpp domain 3
[UPEG-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEG-rrpp-domain-region3] control-vlan 20
[UPEG-rrpp-domain-region3] quit
```

Step 4 Create RRPP rings.

- Configure UPE A.

Configure UPE A as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE A.

```
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port xgigabitethernet
```

```
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

Configure UPE A as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE A.

```
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- # Configure UPE B.

Configure UPE B as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE B.

```
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

Configure UPE B as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE B.

```
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

Configure UPE C as a transit node of ring 1 in domain 1 and specify primary and secondary ports on UPE C.

```
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

Configure UPE C as a transit node of ring 1 in domain 2 and specify primary and secondary ports on UPE C.

```
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

- Configure UPE D.

Configure UPE D as the master node of ring 1 in domain 1. Configure XGE 0/0/1 as the primary port and XGE 0/0/2 as the secondary port.

```
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] ring 1 node-mode master primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPED-rrpp-domain-region1] ring 1 enable
[UPED-rrpp-domain-region1] quit
```

Configure UPE D as the master node of ring 1 in domain 2. Configure XGE 0/0/2 as the primary port and XGE 0/0/1 as the secondary port.

```
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] ring 1 node-mode master primary-port xgigabitethernet
```

```
0/0/2 secondary-port xgigabitethernet 0/0/1 level 0
[UPED-rrpp-domain-region2] ring 1 enable
[UPED-rrpp-domain-region2] quit
```

Configure UPE D as a transit node of ring 1 in domain 3 and specify primary and secondary ports on UPE D.

```
[UPED] rrpp domain 3
[UPED-rrpp-domain-region3] ring 1 node-mode transit primary-port xgigabitethernet
0/0/2 secondary-port xgigabitethernet 0/0/4 level 0
[UPED-rrpp-domain-region3] ring 1 enable
[UPED-rrpp-domain-region3] quit
```

- Configure UPE E.

Configure UPE E as a transit node of ring 1 in domain 3 and specify primary and secondary ports on UPE E.

```
[UPEE] rrpp domain 3
[UPEE-rrpp-domain-region3] ring 1 node-mode transit primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEE-rrpp-domain-region3] ring 1 enable
[UPEE-rrpp-domain-region3] quit
```

- Configure UPE F.

Configure UPE F as the master node of ring 1 in domain 3. Configure XGE 0/0/1 as the primary port and XGE 0/0/2 as the secondary port.

```
[UPEF] rrpp domain 3
[UPEF-rrpp-domain-region3] ring 1 node-mode master primary-port xgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEF-rrpp-domain-region3] ring 1 enable
[UPEF-rrpp-domain-region3] quit
```

- Configure UPE G.

Configure UPE G as a transit node of ring 1 in domain 3 and specify primary and secondary ports on UPE G.

```
[UPEG] rrpp domain 3
[UPEG-rrpp-domain-region3] ring 1 node-mode transit primary-portxgigabitethernet
0/0/1 secondary-port xgigabitethernet 0/0/2 level 0
[UPEG-rrpp-domain-region3] ring 1 enable
[UPEG-rrpp-domain-region3] quit
```

Step 5 Enable the RRPP protocol.

After configuring an RRPP ring, you need to enable RRPP on each node on the ring to activate the RRPP ring. The configuration procedure is as follows:

- Configure UPE A.

Enable the RRPP protocol.

```
[UPEA] rrpp enable
```

- # Configure UPE B.

Enable the RRPP protocol.

```
[UPEB] rrpp enable
```

- Configure UPE C.

Enable the RRPP protocol.

```
[UPEC] rrpp enable
```

- Configure UPE D.

Enable the RRPP protocol.

```
[UPED] rrpp enable
```

- Configure UPE E.

Enable the RRPP protocol.

```
[UPEE] rrpp enable
```

- Configure UPE F.

Enable the RRPP protocol.

```
[UPEF] rrpp enable
```

- Configure UPE G.

Enable the RRPP protocol.

```
[UPEG] rrpp enable
```

Step 6 Verify the configuration.

After the preceding configurations are complete and the network topology becomes stable, perform the following operations to verify the configuration. Here, UPE D is taken for example.

- Run the **display rrpp brief** command on UPE D. The following information is displayed:

```
[UPED] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default).
Number of RRPP Domains: 3

Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 --------------------------------------------------------------------------
 1     0      M     XGigabitEthernet0/0/1     XGigabitEthernet0/0/2     Yes

Domain Index   : 2
Control VLAN   : major 10    sub 11
Protected VLAN : Reference Instance 2
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary                  Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 --------------------------------------------------------------------------
 1     0      M     XGigabitEthernet0/0/2     XGigabitEthernet0/0/1     Yes

Domain Index   : 3
Control VLAN   : major 20    sub 21
Protected VLAN : Reference Instance 1 to 3
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
 Ring  Ring   Node  Primary/Common           Secondary/Edge           Is
 ID    Level  Mode  Port                     Port                     Enabled
 --------------------------------------------------------------------------
 1     0      T     XGigabitEthernet0/0/3     XGigabitEthernet0/0/4     Yes
```

The preceding information shows that the RRPP protocol is enabled on UPE D.

In domain 1:

VLAN 1 is the control VLAN and VLANs mapping instance 1 are the protected VLANs.

UPE D is the master on ring 1; XGE 0/0/1 is the primary port; XGE 0/0/2 is the secondary port.

In domain 2:

VLAN 10 is the control VLAN and VLANs mapping instance 2 are the protected VLANs.

UPE D is the master node on ring 1. The primary port is XGE 0/0/2, and the secondary port is XGE 0/0/1.

In domain 3:

VLAN 20 is the control VLAN and VLANs mapping instance 1 to 3 are the protected VLANs.

UPE D is a transit node on ring 1. The primary port is XGE 0/0/3, and the secondary port is XGE 0/0/4.

- Run the **display rrpp verbose domain** command on UPE D. You can obtain the following results:

View detailed information about UPE D in domain 1.

```
[UPED] display rrpp verbose domain 1
Domain Index   : 1
Control VLAN   : major 5    sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                              Is Active: Yes
Primary port   : XGigabitEthernet0/0/1                Port status: UP
Secondary port : XGigabitEthernet0/0/2                Port status: BLOCKED
```

The preceding information shows that VLAN 1 is the control VLAN in domain 1 and VLANs mapping instance 1 are the protected VLANs.

UPE D is the master node in domain 1 and is in Complete state.

The primary port is XGE 0/0/1, and the secondary port is XGE 0/0/2.

View detailed information about UPE D in domain 2.

```
[UPED] display rrpp verbose domain 2
Domain Index   : 2
Control VLAN   : major 10    sub 11
Protected VLAN : Reference Instance 2
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                              Is Active: Yes
Primary port   : XGigabitEthernet0/0/2                Port status: UP
Secondary port : XGigabitEthernet0/0/1                Port status: BLOCKED
```

The preceding information shows that VLAN 10 is the control VLAN in domain 2, and VLANs mapping instance 2 are the protected VLANs.

UPE D is the master node in domain 2 and is in Complete state.

The primary port is XGE 0/0/2, and the secondary port is XGE 0/0/1.

View detailed information about UPE D in domain 3.

```
[UPED] display rrpp verbose domain 3
Domain Index   : 3
Control VLAN   : major 20    sub 21
Protected VLAN : Reference Instance 1 to 3
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Transit
Ring State     : LinkUp
Is Enabled     : Enable                              Is Active: Yes
Primary port   : XGigabitEthernet0/0/3               Port status: UP
Secondary port : XGigabitEthernet0/0/4               Port status: UP
```

The preceding information shows that VLAN 20 is the control VLAN in domain 3 and VLANs mapping instance 1 to 3 are the protected VLANs.

UPE D is a transit node in domain 3 and is in LinkUp state.

The primary port is XGE 0/0/3, and the secondary port is XGE 0/0/4.

----End

Configuration Files

- Configuration file of UPE A

```
#
sysname UPEA
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE B

```
#
sysname UPEB
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE C

```
#
sysname UPEC
#
vlan batch 5 to 6 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 1
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
```

```
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
Return
```

- Configuration file of UPE D

```
#
sysname UPED
#
vlan batch 5 to 6 10 to 11 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 5 to 6 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 instance 3 vlan 20 to 21
 active region-configuration
#
rrpp domain 1
 control-vlan 5
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/2 secondary-port
XGigabitEthernet 0/0/1 level 0
 ring 1 enable
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1 2 3
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/3 secondary-port
XGigabitEthernet 0/0/4 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 5 to 6 10 to 11 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- Configuration file of UPE E

```
#
sysname UPEE
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
```

```
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- Configuration file of UPE F

```
#
sysname UPEF
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port XGigabitEthernet 0/0/1 secondary-port
XGigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- Configuration file of UPE G

```
#
sysname UPEG
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port XGigabitEthernet 0/0/1 secondary-port
```

```
XGigabitEthernet 0/0/2
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

7.4 Ethernet OAM Configuration-EFM

This chapter describes Ethernet OAM and its configurations, and how to implement link-level Ethernet OAM detection to improve network reliability.

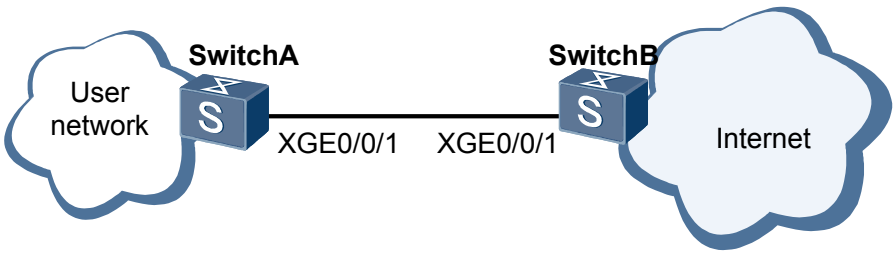
7.4.1 Example for Configuring EFM OAM

Networking Requirements

As shown in **Figure 7-11**, a user network is connected to an ISP network through Switch A and Switch B. Switch A functions as the CE device, and Switch B functions as the underlayer PE (UPE) device. The networking requirements are as follows:

- Automatic connectivity detection can be performed between Switch A and Switch B. After detecting connectivity faults, Switch A and Switch B generate alarms.
- Switch B monitors the errored frames, errored codes, and errored frame seconds on XGE 0/0/1. When the number of errored frames, errored codes, or errored frame seconds exceeds the threshold, Switch B generates an alarm.

Figure 7-11 Networking diagram for configuring EFM OAM



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable EFM OAM globally on Switch A and Switch B.
2. Configure EFM OAM on XGE 0/0/1 of Switch A to work in passive mode.
3. Enable EFM OAM on XGE 0/0/1 on Switch B. Enable EFM OAM on XGE 0/0/1 on Switch A.

4. Configure XGE 0/0/1 of Switch B to detect the errored frames, errored codes, and errored frame seconds.

Data Preparation

To complete the configuration, you need the following data:

- Period for detecting errored frames on XGE 0/0/1 of Switch B (5 seconds) and threshold of number of errored frames (5)
- Period for detecting errored codes on XGE 0/0/1 of Switch B (5 seconds) and threshold of number of errored codes (5)
- Period for detecting errored frame seconds on XGE 0/0/1 of Switch B (120 seconds) and threshold of number of errored frame seconds (5)

Procedure

Step 1 Enable EFM OAM globally.

Enable EFM OAM globally on Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] efm enable
```

Enable EFM OAM globally on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] efm enable
```

Step 2 Configure EFM OAM on XGE 0/0/1 of Switch A to work in passive mode.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] efm mode passive
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
```

Step 3 Enable EFM OAM on XGE 0/0/1 of Switch B and XGE 0/0/1 of Switch A.

Enable EFM OAM on XGE 0/0/1 of Switch A.

```
[SwitchA-XGigabitEthernet0/0/1] efm enable
[SwitchA-XGigabitEthernet0/0/1] quit
```

Enable EFM OAM of XGE 0/0/1 on Switch B.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] efm enable
[SwitchB-XGigabitEthernet0/0/1] bpdu enable
```

Step 4 Configure XGE 0/0/1 of Switch B to detect the errored frames, errored codes, and errored frame seconds.

Configure XGE 0/0/1 of Switch B to detect the errored frames.

```
[SwitchB-XGigabitEthernet0/0/1] efm error-frame period 5
[SwitchB-XGigabitEthernet0/0/1] efm error-frame threshold 5
[SwitchB-XGigabitEthernet0/0/1] efm error-frame notification enable
```

Configure XGE 0/0/1 of Switch B to detect the errored codes.

```
[SwitchB-XGigabitEthernet0/0/1] efm error-code period 5
[SwitchB-XGigabitEthernet0/0/1] efm error-code threshold 5
[SwitchB-XGigabitEthernet0/0/1] efm error-code notification enable
```

Configure n XGE 0/0/1 of Switch B to detect the errored frames seconds.

```
[SwitchB-XGigabitEthernet0/0/1] efm error-frame-second period 120
[SwitchB-XGigabitEthernet0/0/1] efm error-frame-second threshold 5
[SwitchB-XGigabitEthernet0/0/1] efm error-frame-second notification enable
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 5 Verify the configuration.

If EFM OAM is configured correctly on Switch A and Switch B, XGE 0/0/1 and XGE 0/0/1 start the handshake after negotiation. Run the **display efm session** command on Switch A or Switch B, and you can find that the EFM OAM protocol is in detect state.

```
[SwitchB] display efm session interface gigabitethernet 0/0/1
  Interface               EFM State               Loopback Timeout
  ------------------------------------------------------------------
  XGigabitEthernet0/0/1    detect                  --
```

Run the **display efm** command on Switch B. If the function of detecting errored frames, errored codes, and errored frame seconds on XGE 0/0/1 is configured corrected, the following information is displayed:

```
[SwitchB] display efm interface xgigabitethernet 0/0/1
    Item                          Value
    ------------------------------------
    Interface:                    XGigabitEthernet0/0/1
    EFM Enable Flag:              enable
    Mode:                         active
    OAMPDU MaxSize:               128
    ErrCodeNotification:          enable
    ErrCodePeriod:                5
    ErrCodeThreshold:             5
    ErrFrameNotification:         enable
    ErrFramePeriod:               5
    ErrFrameThreshold:            5
    ErrFrameSecondNotification:   enable
    ErrFrameSecondPeriod:         120
    ErrFrameSecondThreshold:      5
    Hold Up Time:                 10
    ThresholdEvtTriggerErrDown:   enable
    TriggerIfDown:                disable
    TriggerMacRenew:              disable
    Remote MAC:                   0010-0010-0010
    Remote EFM Enable Flag:       enable
    Remote Mode:                  passive
    Remote  MaxSize:              128
    Remote State:                   --
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
 efm enable
#
 interface XGigabitEthernet0/0/1
 efm mode passive
 efm enable
#
return
```

- Configuration file of Switch B

```
#
sysname SwitchB
#
 efm enable
```

```
#
interface XGigabitEthernet0/0/1
 efm enable
 efm error-frame period 5
 efm error-frame threshold 5
 efm error-frame notification enable
 efm error-frame-second period 120
 efm error-frame-second threshold 5
 efm error-frame-second notification enable
 efm error-code period 5
 efm error-code threshold 5
 efm error-code notification enable
#
return
```

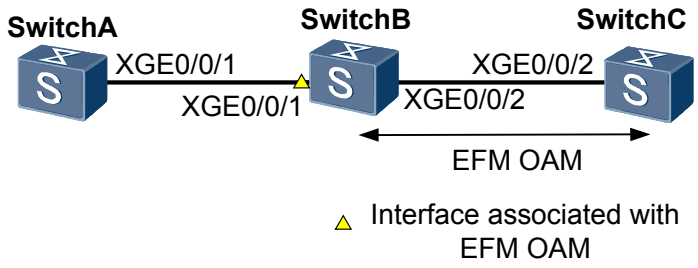
7.4.2 Example for Configuring Association Between an EFM OAM Module and an Interface

If association between an EFM OAM module and an interface is configured on a device, when the EFM OAM module detects a fault, the EFM OAM module on the local device sends a fault notification message to the OAM management module and triggers the physical status of the interface bound to the EFM OAM module to go Down. When the physical status of the interface becomes Down, the OAM management module sends a fault notification message to the EFM OAM module. Then the EFM OAM module sends the fault notification message to the remote device.

Networking Requirements

As shown in **Figure 7-12**, EFM OAM is configured between Switch B and Switch C. When XGE 0/0/2 on Switch B becomes Down, the EFM OAM module reports the fault to XGE 0/0/1 on Switch C through the association mechanism. Then XGE 0/0/1 is triggered to go Down.

Figure 7-12 Networking diagram for configuring association between an EFM OAM module and an interface



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure EFM OAM between Switch B and Switch C.
2. On Switch B, configure association between an EFM OAM module and XGE 0/0/1.

Procedure

Step 1 Configure EFM OAM between Switch B and Switch C.

Configure Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] efm enable
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] bpdu enable
[SwitchB-XGigabitEthernet0/0/2] efm mode passive
[SwitchB-XGigabitEthernet0/0/2] efm enable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Configure Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] efm enable
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] bpdu enable
[SwitchC-XGigabitEthernet0/0/2] efm enable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Run the **display efm session interface** command on Switch B to check the EFM OAM status, and you can find that EFM OAM is in **detect** state.

```
[SwitchB] display efm session interface xgigabitethernet 0/0/2
  Interface               EFM State               Loopback Timeout
  ------------------------------------------------------------------
  XGigabitEthernet0/0/2    detect              --
```

Step 2 Configure association between an EFM OAM module with an interface.

Enable XGE 0/0/1 on Switch B and the EFM OAM module between Switch B and Switch C to report faults to each other.

```
[SwitchB] oam-mgr
[SwitchB-oam-mgr] oam-bind efm interface xgigabitethernet 0/0/2 trigger if-down
interface xgigabitethernet 0/0/1
[SwitchB-oam-mgr] quit
```

Step 3 Verify the configuration.

After XGE 0/0/2 on Switch B is shut down, the EFM OAM module reports the fault to XGE 0/0/1. Then XGE 0/0/1 is triggered to go Down.

```
[SwitchB] display interface xgigabitethernet 0/0/1
XGigabitEthernet0/0/1 current state : TRIGGER DOWN
(3AH)
Line protocol current state : DOWN
Description:HUAWEI, Quidway Series, XGigabitEthernet0/0/1 Interface
Switch Port,PVID :    1,The Maximum Frame Length is 1600
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-8211-1111
Port Mode: COMBO AUTO
Current Work Mode: COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -
Input:  0 packets, 0 bytes
Unicast        :                  0,Multicast          :                  0
Broadcast      :                  0,Jumbo              :                  0
CRC            :                  0,Giants             :                  0
```

```
Jabbers         :                   0,Throttles          :                   0
Runts           :                   0,DropEvents         :                   0
Alignments      :                   0,Symbols            :                   0
Ignoreds        :                   0,Frames             :                   0
Discard         :                   0,Total Error        :                   0
Output:  0 packets, 0 bytes
Unicast         :                   0,Multicast          :                   0
Broadcast       :                   0,Jumbo              :                   0
Collisions      :                   0,Deferreds          :                   0
Late Collisions:                    0,ExcessiveCollisions:                  0
Buffers Purged :                    0
Discard         :                   0,Total Error        :                   0
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

----End

Configuration Files

- Configuration file of Switch B

```
#
 sysname SwitchB
#
efm enable
#
interface XGigabitEthernet0/0/1
 efm enable
#
interface XGigabitEthernet0/0/2
 efm mode passive
 efm enable
 bpdu enable
#
 oam-mgr
  oam-bind ingress interface XGigabitEthernet0/0/2 egress efm interface
XGigabitEthernet0/0/1 trigger if-
down
  oam-bind ingress efm interface XGigabitEthernet0/0/1 trigger if-down egress
interface XGigabitEthernet0/0/2
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
efm enable
#
interface XGigabitEthernet0/0/2
 efm enable
 bpdu enable
#
return
```

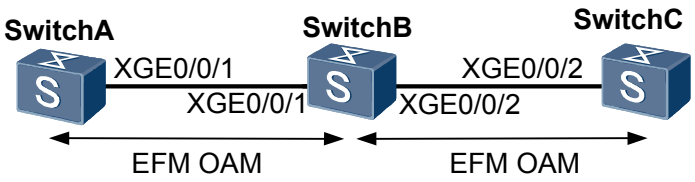
7.4.3 Example for Configuring Association Between EFM OAM Modules

Networking Requirements

As shown in **Figure 7-13**, to implement the end-to-end link fault detection, EFM OAM is configured between Switch A and Switch B and between Switch B and Switch C. When a fault occurs on the link between Switch A and Switch B, EFM OAM between Switch A and Switch

B detects the fault and sends fault messages to Switch C through the association mechanism. Then, alarms are generated on Switch C.

Figure 7-13 Networking diagram for configuring association between EFM OAM modules



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable EFM OAM globally on Switch A, Switch B, and Switch C.
2. Configure EFM OAM on XGE 0/0/1 of Switch B and XGE 0/0/2 of Switch C to work in passive mode.
3. Enable EFM OAM on interfaces of the S6700s.
4. Configure association between EFM OAM modules on Switch B.

Procedure

Step 1 Enable EFM OAM globally.

Configure Switch A.

```
<SwitchA> system-view
[SwitchA] efm enable
```

Configure SwitchB.

```
<SwitchB> system-view
[SwitchB] efm enable
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] efm enable
```

Step 2 Configure the operation mode of interfaces.

Configure Switch B.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] bpdu enable
[SwitchB-XGigabitEthernet0/0/1] efm mode passive
[SwitchB-XGigabitEthernet0/0/1] quit
```

Configure SwitchC.

```
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] bpdu enable
[SwitchC-XGigabitEthernet0/0/2] efm mode passive
[SwitchC-XGigabitEthernet0/0/2] quit
```

Step 3 Enable EFM OAM on interfaces.

Configure Switch A.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
```

```
[SwitchA-XGigabitEthernet0/0/1] efm enable
[SwitchA-XGigabitEthernet0/0/1] quit
```

Configure Switch B.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] efm enable
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet 0/0/2
[SwitchB-XGigabitEthernet0/0/2] bpdu enable
[SwitchB-XGigabitEthernet0/0/2] efm enable
[SwitchB-XGigabitEthernet0/0/2] quit
```

Configure Switch C.

```
[SwitchC] interface xgigabitethernet 0/0/2
[SwitchC-XGigabitEthernet0/0/2] efm enable
[SwitchC-XGigabitEthernet0/0/2] quit
```

Run the **display efm session all** command to check the EFM OAM status, and you can find that EFM OAM is in **detect** state. Take the display on Switch B as an example.

```
[SwitchB] display efm session all
  Interface                EFM State                   Loopback Timeout
  ------------------------------------------------------------------------
  XGigabitEthernet0/0/1      detect                     --
  XGigabitEthernet0/0/2      detect                     --
```

Step 4 Configure association between EFM OAM modules.

```
[SwitchB] oam-mgr
[SwitchB-oam-mgr] oam-bind efm interface xgigabitethernet 0/0/1 efm interface
xgigabitethernet 0/0/2
```

In the OAM management view, run the **display this** command to check association. You can find that there are two unidirectional association configuration records, whose directions are mutually reverse.

```
[SwitchB-oam-mgr] display this
#
oam-mgr
 oam-bind ingress efm interface XGigabitEthernet0/0/1 egress efm interface
XGigabitEthernet0/0/2
 oam-bind ingress efm interface XGigabitEthernet0/0/2 egress efm interface
XGigabitEthernet0/0/1
#
```

Step 5 Verify the configuration.

On SwitchC, enable the function of sending debugging information to a terminal.

```
<SwitchC> terminal logging
<SwitchC> terminal monitor
```

Shut down XGE 0/0/1 on SwitchA and simulate link faults.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] shutdown
```

Fault messages between SwitchA and SwitchB are transmitted to SwitchC through the association mechanism. Then alarms are generated on SwitchC.

```
<SwitchC>
 Mar  9 2010 14:52:33 SwitchC %%01EFM/2/NONTHRESHOLD(l): OID 1.3.6.1.4.1.2011.5
.25.136.1.6.5 Non-threshold-crossing event occurred.
(InterfaceName=XGigabitEthernet0/0/1, EventLogIndex=0,
EventLogTimestamp=148983996, EventLogOui=[01.80.c2 (h
ex)], EventLogType=258, EventLogLocation=2, EventLogRunningTotal=0 3)
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 efm
#
interface XGigabitEthernet0/0/1
 efm enable
 bpdu enable
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 efm
#
interface XGigabitEthernet0/0/1
 efm mode passive
 efm enable
#
interface XGigabitEthernet0/0/2
 efm enable
 bpdu enable
#
oam-mgr
 oam-bind ingress efm interface XGigabitEthernet0/0/1 egress efm interface
XGigabitEthernet0/0/2
 oam-bind ingress efm interface XGigabitEthernet0/0/2 egress efm interface
XGigabitEthernet0/0/1
#
 return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 efm
#
interface XGigabitEthernet0/0/2
 efm mode passive
 efm enable
 bpdu enable
#
return
```

7.5 BFD Configuration

A BFD session rapidly detects a link fault on a network.

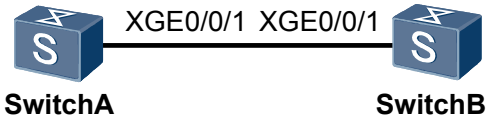
7.5.1 Example for Configuring Single-Hop BFD on a Layer 2 Interface

Networking Requirements

Interfaces of the S6700 are Layer 2 interfaces. If you need to detect the connectivity of the Layer 2 forwarding link between two directly connected S6700s, configure single-hop BFD, and bind the BFD session to a multicast IP address and local interface.

As shown in **Figure 7-14**, a BFD session is created to detect the connectivity of the Layer 2 link between Switch A and Switch B.

Figure 7-14 Networking diagram of single-hop BFD (for Layer 2 forwarding link)



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a BFD session on Switch A to detect the direct link from Switch A to Switch B.
2. Configure a BFD session on Switch B to detect the direct link from Switch B to Switch A.

Data Preparation

To complete the configuration, you need the following data:

- Type and number of the interface bound to the BFD session
- Local and remote identifiers of the BFD session

Use the default values of the minimum sending interval, the minimum receiving interval, and the local detection multiplier of BFD control packets.

Procedure

Step 1 Configure single-hop BFD on Switch A.

Enable BFD on Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] bfd
[SwitchA-bfd] quit
```

Create a BFD session on Switch A.

```
[SwitchA] bfd atob bind peer-ip default-ip interface xgigabitethernet 0/0/1
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

Step 2 Configure single-hop BFD on Switch B.

Enable BFD on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] bfd
[SwitchB-bfd] quit
```

Create a BFD session on Switch B.

```
[SwitchB] bfd btoa bind peer-ip default-ip interface xgigabitethernet 0/0/1
[SwitchB-bfd-session-btoa] discriminator local 2
```

```
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

Step 3 Verify the configuration.

After the configuration, run the **display bfd session** command on Switch A and Switch B, and you can find that a single-hop BFD session is set up and is in Up state.

Take Switch A for example. The display is as follows:

```
<SwitchA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4097      (One Hop) State : Up        Name : atob
--------------------------------------------------------------------------------
  Local Discriminator    : 1              Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(XGigabitEthernet0/0/1)
  Bind Session Type      : Static
  Bind Peer IP Address   : 224.0.0.184
  NextHop Ip Address     : 224.0.0.184
  Bind Interface         : XGigabitEthernet0/0/1
  FSM Board Id           : 0                TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3                Detect Interval (ms)   : 3000
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 255
  Proc Interface Status  : Disable
  WTR Interval (ms)      : -
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : -                Session Detect TmrID   : -
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
--------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 1/0
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 bfd
#
bfd atob bind peer-ip default-ip interface XGigabitEthernet0/0/1
 discriminator local 1
 discriminator remote 2
 commit
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 bfd
#
bfd btoa bind peer-ip default-ip interface XGigabitEthernet0/0/1
 discriminator local 2
 discriminator remote 1
```

```
 commit
#
return
```

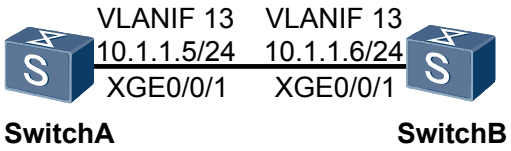
7.5.2 Example for Configuring Single-Hop BFD on a VLANIF Interface

Networking Requirements

The S6700s are connected through the VLANIF interface at Layer 3. To detect the connectivity of the link between two directly connected S6700s, you can configure single-hop BFD to bind the BFD session to the VLANIF interface and its IP address.

As shown in **Figure 7-15**, a BFD session is created to detect the connectivity of the link between Switch A and Switch B.

Figure 7-15 Networking diagram for configuring single-hop BFD on a VLANIF interface



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLAN 13 on Switch A and Switch B.
2. Configure XGE 0/0/1 interfaces on Switch A and Switch B as hybrid interfaces.
3. Create VLANIF 13 on Switch A and Switch B and set their IP address.
4. Create a BFD session on Switch A to detect the link between Switch A and Switch B.
5. Create a BFD session on Switch B to detect the link between Switch B and Switch A.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of VLANIF interfaces bound to BFD sessions
- IP addresses of VLANIF interfaces
- Local and remote discriminators of BFD sessions

Default values of minimum intervals for sending BFD control packets, minimum intervals for receiving BFD control packets, and local detection multipliers

Procedure

Step 1 On Switch A and Switch B, create VLAN 13, configure XGE 0/0/1 interfaces as hybrid interfaces, and add XGE 0/0/1 interfaces to VLAN 13.

Configure Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 13
[SwitchA-vlan13] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 13
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 13
[SwitchA-XGigabitEthernet0/0/1] quit
```

Configure SwitchB.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 13
[SwitchB-vlan13] quit
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid pvid vlan 13
[SwitchB-XGigabitEthernet0/0/1] port hybrid untagged vlan 13
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 2 Set IP addresses of VLANIF 13 interfaces so that Switch A can communicate with Switch B at Layer 3.

Configure Switch A.

```
[SwitchA] interface vlanif13
[SwitchA-Vlanif13] ip address 10.1.1.5 24
[SwitchA-Vlanif13] quit
```

Configure Switch B.

```
[SwitchB] interface vlanif13
[SwitchB-Vlanif13] ip address 10.1.1.6 24
[SwitchB-Vlanif13] quit
```

After the configuration, run the **display interface vlanif** command on Switch A or Switch B. You can view that the status of VLANIF 13 is Up.

```
[SwitchA] display interface vlanif 13
Vlanif13 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif13 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-827d-75f5
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 3 Configure single-hop BFD on Switch A.

Enable BFD on Switch A.

```
[SwitchA] bfd
[SwitchA-bfd] quit
```

Create a BFD session on SwitchA.

```
[SwitchA] bfd atob bind peer-ip 10.1.1.6 interface vlanif 13
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

Step 4 Configure single-hop BFD on Switch B.

Enable BFD on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] bfd
[SwitchB-bfd] quit
```

Create a BFD session on Switch B.

```
[SwitchB] bfd btoa bind peer-ip 10.1.1.5 interface vlanif 13
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

Step 5 Verify the configuration.

After the configuration, run the **display bfd session** command on Switch A and Switch B. You can view that the single-hop BFD session is set up and the status is Up.

Take the display on Switch A as an example.

```
<SwitchA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4097      (One Hop) State : Up        Name : atob
--------------------------------------------------------------------------------
  Local Discriminator    : 1               Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(Vlanif13)
  Bind Session Type      : Static
  Bind Peer IP Address   : 10.1.1.6
  Bind Interface         : Vlanif13
  FSM Board Id           : 0               TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000            Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3               Detect Interval (ms)   : -
  Echo Passive           : Disable         Acl Number             : -
  Destination Port       : 3784            TTL                    : 255
  Proc Interface Status  : Disable
  WTR Interval (ms)      : -
  Active Multi           : -
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : 16392           Session Detect TmrID   : -
  Session Init TmrID     : -               Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
--------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 0/1
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 13
#
 bfd
#
interface Vlanif13
 ip address 10.1.1.5 255.255.255.0
#
```

```
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
#
bfd atob bind peer-ip 10.1.1.6 interface Vlanif13
 discriminator local 1
 discriminator remote 2
 commit
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 13
#
 bfd
#
interface Vlanif13
 ip address 10.1.1.6 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
#
bfd btoa bind peer-ip 10.1.1.5 interface Vlanif13
 discriminator local 2
 discriminator remote 1
 commit
#
return
```

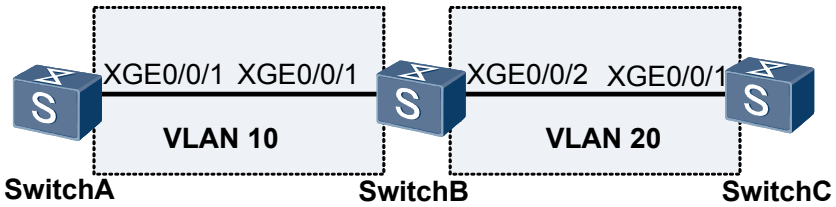
7.5.3 Example for Configuring Multi-Hop BFD

Networking Requirements

As shown in **Figure 7-16**, a BFD session is used to test the multi-hop path between Switch A and Switch C.

Interfaces of the S6700 are Layer 2 interfaces. To configure multi-hop BFD, you need to add an interface to a VLAN, create a VLANIF interface, and assign an IP address to the VLANIF interface.

Figure 7-16 Networking diagram of multi-hop BFD



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a BFD session on Switch A to detect the multi-hop path from Switch A to Switch C.
2. Configure a BFD session on Switch C to detect the multi-hop path from Switch C to Switch A.

Data Preparation

To complete the configuration, you need the following data:

- Peer IP address bound to the BFD session
- Local and remote identifiers of the BFD session
- IP address of VLANIF 10 on Switch A: 10.1.1.1/16
- IP address of VLANIF 10 on Switch B: 10.1.1.2/16
- IP address of VLANIF 20 on Switch B: 10.2.1.1/16
- IP address of VLANIF 20 on Switch C: 10.2.1.2/16

Use the default values of the minimum sending interval, the minimum receiving interval, and the local detection multiplier of a BFD control packet.

Procedure

Step 1 Add interfaces to VLANs, create VLANIF interfaces, and assign an IP address to each VLANIF interface.

Create a VLAN on Switch A and add the interface to the VLAN.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 10
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
```

Create a VLANIF interface and assign an IP address to the VLANIF interface.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 16
[SwitchA-Vlanif10] quit
```

The configurations of Switch B and Switch C are the same as the configuration of Switch A, and are not mentioned here.

Step 2 Configure a reachable static route between Switch A and Switch C.

```
[SwitchA] ip route-static 10.2.0.0 16 10.1.1.2
```

The configuration of Switch C is the same as the configuration of Switch A, and is not mentioned here.

Step 3 Configure multi-hop BFD on Switch A and Switch C.

Create a BFD session with Switch C on Switch A.

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atoc bind peer-ip 10.2.1.2
[SwitchA-bfd-session-atoc] discriminator local 10
[SwitchA-bfd-session-atoc] discriminator remote 20
[SwitchA-bfd-session-atoc] commit
[SwitchA-bfd-session-atoc] quit
```

Create a BFD session with Switch A on Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] bfd
[SwitchC-bfd] quit
[SwitchC] bfd ctoa bind peer-ip 10.1.1.1
[SwitchC-bfd-session-ctoa] discriminator local 20
[SwitchC-bfd-session-ctoa] discriminator remote 10
[SwitchC-bfd-session-ctoa] commit
[SwitchC-bfd-session-ctoa] quit
```

Step 4 Verify the configuration.

After the configuration is complete, run the **display bfd session** command on Switch A and Switch C, and you can find that a BFD session is set up and is in Up state.

Take Switch A for example. The display is as follows:

```
<SwitchA> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4096      (Multi Hop) State : Up        Name : atoc
--------------------------------------------------------------------------------
  Local Discriminator    : 10              Remote Discriminator   : 20
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address
  Bind Session Type      : Static
  Bind Peer IP Address   : 10.2.1.2
  Bind Interface         : -
  FSM Board Id           : 0               TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000            Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000            Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3               Detect Interval (ms)   : 3000
  Echo Passive           : Disable         Acl Number             : -
  Destination Port       : 3784            TTL                    : 255
  Proc Interface Status  : Disable
  WTR Interval (ms)      : -
  Active Multi           : 3
  Last Local Diagnostic  : Control Detection Time Expired
  Bind Application       : No Application Bind
  Session TX TmrID       : 16445           Session Detect TmrID   : -
  Session Init TmrID     : 16447           Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
--------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 0/1
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10
#
 bfd
#
interface Vlanif10
 ip address 10.1.1.1 255.255.0.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
```

```
#
bfd atoc bind peer-ip 10.2.1.2
 discriminator local 10
 discriminator remote 20
 commit
#
 ip route-static 10.2.0.0 255.255.0.0 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.1.1.2 255.255.0.0
#
interface Vlanif20
 ip address 10.2.1.1 255.255.0.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 bfd
#
 vlan batch 20
#
interface Vlanif20
 ip address 10.2.1.2 255.255.0.0
#
interface XGigabitEthernet0/0/1
  port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
bfd ctoa bind peer-ip 10.1.1.1
 discriminator local 20
 discriminator remote 10
 commit
#
 ip route-static 10.1.0.0 255.255.0.0 10.2.1.1
#
return
```

7.6 VRRP and VRRP6 Configuration

A VRRPor VRRP6 backup group allows a backup to take over network traffic from a master if the master fails.

7.6.1 Example for Configuring VRRP in Master/Backup Mode

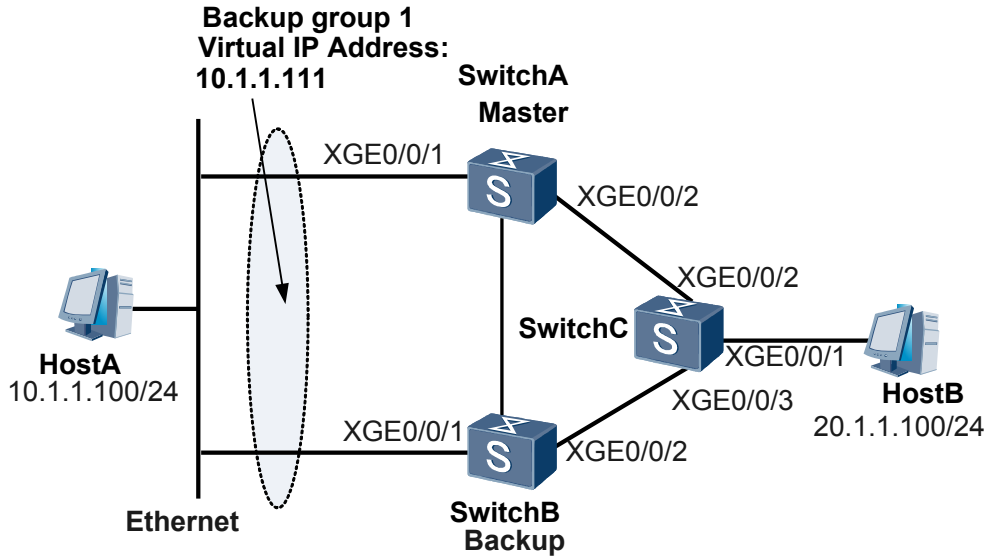
Networking Requirements

As shown in **Figure 7-17**, Host A communicates with Host B through the default gateway.

The requirements are as follows:

- The VRRP group that consists of SwitchA and SwitchB functions as the default gateway of Host A.
- SwitchA functions as the gateway. When SwitchA fails, SwitchB becomes the gateway.
- After SwitchA recovers, it preempts to be the master router within 20 seconds.

Figure 7-17 Networking of a VRRP group in master/backup mode



Device	Interface	VLANIF interface	IP address
SwitchA	XGE 0/0/1	VLANIF100	10.1.1.1/24
	XGE 0/0/2	VLANIF200	192.168.1.1/24
SwitchB	XGE 0/0/1	VLANIF100	10.1.1.2/24
	XGE 0/0/2	VLANIF400	192.168.2.1/24
SwitchC	XGE 0/0/1	VLANIF300	20.1.1.1/24
	XGE 0/0/2	VLANIF200	192.168.1.2/24
	XGE 0/0/3	VLANIF400	192.168.2.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure VLANIF interfaces and assign IP addresses to the VLANIF interface.
2. Configure the OSPF protocol between Switch A, Switch B, and Switch C to implement interworking between them.
3. Create VRRP group 1 on VLANIF 100 of Switch A. Set the highest priority for Switch A in the VRRP group to ensure that Switch A functions as the master. Configure the preemption mode on Switch A.
4. Create VRRP group 1 on VLANIF 100 of Switch B and use the default priority.

Data Preparation

To complete the configuration, you need the following data:

- ID and virtual IP address of the VRRP group
- Priorities of Switch A and Switch B in the VRRP group
- Preemption mode

Procedure

Step 1 Configure VLANIF interfaces and assign IP addresses to the VLANIF interface.

Create VLANs and add physical interfaces to VLANs.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100 200
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-XGigabitEthernet0/0/1] quit
```

The configurations of Switch B and Switch C are similar to the configuration of Switch A, and are not mentioned here.

Configure an IP address for the VLANIF interface on SwitchA.

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] ip address 192.168.1.1 24
[SwitchA-Vlanif200] quit
```

Configure an IP address for the VLANIF interface on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 400
[SwitchB-Vlanif400] ip address 192.168.2.1 24
[SwitchB-Vlanif400] quit
```

Configure an IP address for the VLANIF interface on Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
```

```
[SwitchC] interface vlanif 200
[SwitchC-Vlanif200] ip address 192.168.1.2 24
[SwitchC-Vlanif200] quit
[SwitchC] interface vlanif 300
[SwitchC-Vlanif300] ip address 20.1.1.1 24
[SwitchC-Vlanif300] quit
[SwitchC] interface vlanif 400
[SwitchC-Vlanif400] ip address 192.168.2.2 24
[SwitchC-Vlanif400] quit
```

Step 2 Configure the OSPF protocol between Switch A, Switch B, and Switch C.

Configure Switch A.

```
[SwitchA] ospf 1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure Switch B.

```
[SwitchB]
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure Switch C.

```
[SwitchC]
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure the default gateway address of Host A to 10.1.1.111 and the default gateway address of Host B to 20.1.1.1.

Step 3 Configure a VRRP group.

On Switch A, assign an IP address to the VLANIF interface. Create VRRP group 1 and set the priority of Switch A in the VRRP group to 120 so that Switch A functions as the master.

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

On Switch B, assign an IP address to the VLANIF interface. Create VRRP group 1 and retain the default priority of SwitchB in the VRRP group so that Switch B functions as the backup.

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

Step 4 Verify the configuration.

- The VRRP group can function as the gateway.

After the preceding configuration, Host A can ping Host B. Run the **display vrrp** command on Switch A, and you can find that Switch A is the master switch. Run the **display vrrp** command on Switch B, and you can find that Switch B is the backup switch.

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 1
    state : Master
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 20
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 1
    state : Backup
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.1
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

Run the **display ip routing-table** command on Switch A and Switch B. You can find a direct route to the virtual IP address in the routing table of Switch A. In the routing table of Switch B, this direct route is an OSPF route. The displayed information on Switch A and Switch B is as follows:

```
[SwitchA] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9       Routes : 10
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
       10.1.1.0/24  Direct 0    0           D  10.1.1.1        Vlanif100
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       20.1.1.0/24  OSPF   10   2           D  192.168.1.2     Vlanif200
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct 0    0           D  192.168.1.1     Vlanif200
    192.168.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.1.2/32  Direct 0    0           D  192.168.1.2     Vlanif200
    192.168.2.0/24  OSPF   10   2           D  10.1.1.2        Vlanif100
[SwitchB] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9       Routes : 10
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
       10.1.1.0/24  Direct 0    0           D  10.1.1.2        Vlanif100
       10.1.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       20.1.1.0/24  OSPF   10   2           D  192.168.2.2     Vlanif200
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF   10   2           D  10.1.1.1        Vlanif100
    192.168.2.0/24  Direct 0    0           D  192.168.2.1     Vlanif200
    192.168.2.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
    192.168.2.2/32  Direct 0    0           D  192.168.2.2     Vlanif200
```

- When Switch A fails, Switch B becomes the master switch.

Run the **shutdown** command on VLANIF 100 of Switch A to simulate a link fault.

Run the **display vrrp** command on Switch B to view information about the VRRP status. You can find that Switch B is the master switch.

```
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 1
    state : Master
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

- When Switch A recovers, it preempts to be the master.

Run the **undo shutdown** command on VLANIF 100 of Switch A. Wait for 20 seconds after VLANIF 100 recovers to the Up state, and then run the **display vrrp** command on Switch A to view the VRRP status. You can find that Switch A is the master switch.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 100 200
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
#
interface Vlanif200
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
```

```
#
 vlan batch 100 400
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
#
interface Vlanif400
 ip address 192.168.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
interface Vlanif200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif300
 ip address 20.1.1.1 255.255.255.0
#
interface Vlanif400
 ip address 192.168.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
return
```

7.6.2 Example for Configuring VRRP in Load Balancing Mode

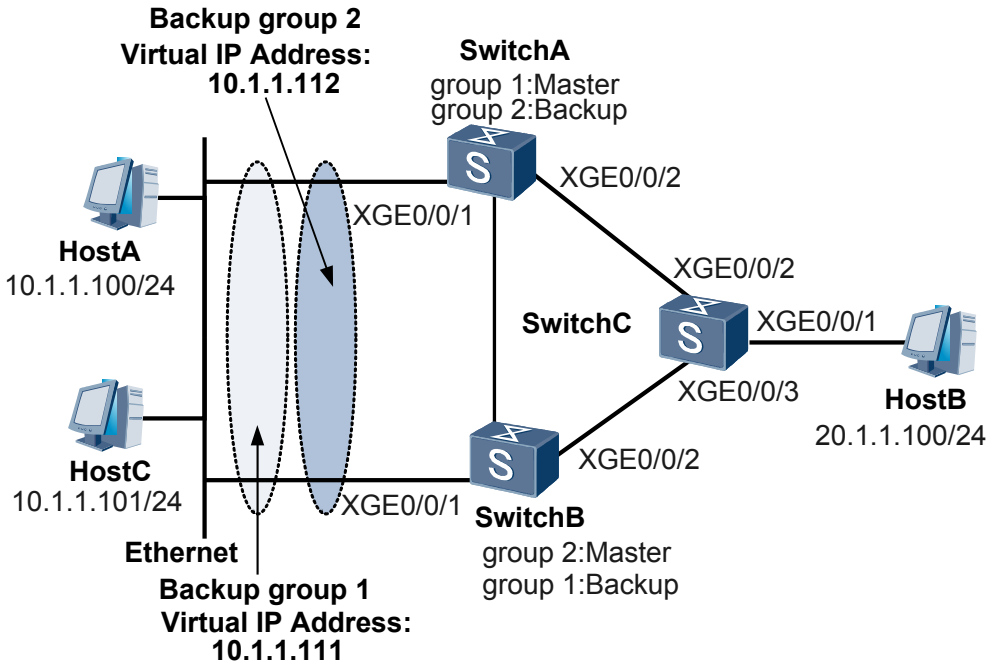
Networking Requirements

As shown in **Figure 7-18**,

- Switch A is the master device in VRRP group 1 and the backup device in VRRP group 2.

- Switch B is the master device in VRRP group 2 and the backup device in VRRP group 1.
- Host A on the internal network uses VRRP group 1 as the gateway, and Host C uses VRRP group 2 as the gateway. The VRRP groups share data flows and back up each other.

Figure 7-18 Networking of VRRP in load balancing mode



Device	Interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF100	10.1.1.1/24
	XGE 0/0/2	VLANIF200	192.168.1.1/24
Switch B	XGE 0/0/1	VLANIF100	10.1.1.2/24
	XGE 0/0/2	VLANIF400	192.168.2.1/24
Switch C	XGE 0/0/1	VLANIF300	20.1.1.1/24
	XGE 0/0/2	VLANIF200	192.168.1.2/24
	XGE 0/0/3	VLANIF400	192.168.2.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Implement networking between Switch A, Switch B, and Switch C.
2. Create two VRRP groups on VLANIF 100 of Switch A. Configure Switch A as the master device in VRRP group 1 and the backup device in VRRP group 2.

3. Create two VRRP groups on VLANIF 100 of Switch B. Configure Switch B as the master device in VRRP group 2 and the backup device in VRRP group 1.

Data Preparation

To complete the configuration, you need the following data:

- IDs and virtual IP addresses of the VRRP groups
- Priorities of Switch A and Switch B in the VRRP groups

Procedure

Step 1 Configure interworking between devices on the network.

Configure the default gateway of Host A to the virtual IP address 10.1.1.111 of VRRP group 1, the default gateway of Host B to 20.1.1.1, and the default gateway of Host C to the virtual IP address 10.1.1.112 of VRRP group 2.

Configure OSPF between Switch A, Switch B, and Switch C.

For details, see **3.4 OSPF Configuration**.

Step 2 Configure VRRP groups.

On Switch A, assign an IP address to VLANIF 100. Create VRRP group 1 and set the priority of Switch A in VRRP group 1 to 120 so that Switch A functions as the master. Create VRRP group 2 and retain the default priority (100) of Switch A in VRRP group 2 so that Switch A functions as the backup device in VRRP group 2.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchA-Vlanif100] quit
```

On Switch B, assign an IP address to VLANIF 100. Create VRRP group 1 and retain the default priority (100) of Switch B in VRRP group 1 so that Switch B functions as the backup. # Create VRRP group 2 on Switch B and set the priority of Switch B in VRRP group 2 to 120 so that Switch B functions as the master in VRRP group 2.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchB-Vlanif100] vrrp vrid 2 priority 120
[SwitchB-Vlanif100] quit
```

Step 3 Verify the configuration.

After the preceding configuration, Host A and Host C can ping Host B successfully.

Tracert Host B from Host A and Host C. Packets from Host A to Host B pass through Switch A and Switch C. Packets from Host C to Host B pass through Switch B and Switch C. That is, load balancing is implemented between Switch A and Switch B.

```
<HostA> tracert 20.1.1.100
 traceroute to  20.1.1.100(20.1.1.100) 30 hops max,40 bytes packet
```

```
 1 10.1.1.1 120 ms  50 ms  60 ms
 2 192.168.1.2 100 ms  60 ms  60 ms
 3 20.1.1.100 130 ms  90 ms  90 ms
<HostC> tracert 20.1.1.100
 traceroute to  20.1.1.100(20.1.1.100) 30 hops max,40 bytes packet
 1 10.1.1.2 30 ms  60 ms  40 ms
 2 192.168.2.2 90 ms  60 ms  60 ms
 3 20.1.1.100 70 ms  60 ms  90 ms
```

Run the **display vrrp** command on Switch A, you can find that Switch A is the master in VRRP group 1 and the backup in VRRP group 2.

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 1
    state : Master
    Virtual IP : 10.1.1.111
    Master IP : 10.1.1.1
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
Vlanif100 | Virtual Router 2
    state : Backup
    Virtual IP : 10.1.1.112
    Master IP : 10.1.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 100 200
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 2 virtual-ip 10.1.1.112
#
interface Vlanif200
 ip address 192.168.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
```

```
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 100 400
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 2 virtual-ip 10.1.1.112
 vrrp vrid 2 priority 120
#
interface Vlanif200
 ip address 192.168.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
interface Vlanif200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif300
 ip address 20.1.1.1 255.255.255.0
#
interface Vlanif400
 ip address 192.168.2.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
```

```
  network 192.168.2.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
return
```

7.6.3 Example for Configuring VRRP Fast Switchover

Networking Requirements

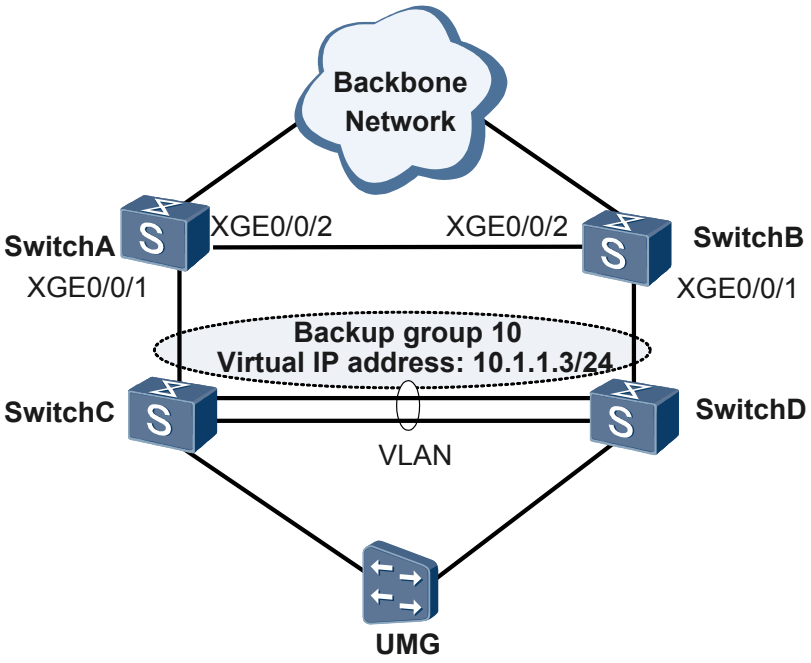
As shown in **Figure 7-19**, Switch A, Switch B, Switch C, Switch D and the Universal Medium Gateway (UMG) form a simple next generation network (NGN).

The networking is as follows:

- The UMG connects to Switch A and Switch B through Switch C and Switch D.
- Switch A and Switch B run VRRP. Switch A functions as the master, and Switch B functions as the backup.

When Switch A fails, or when the link between Switch A and Switch B fails, the active/standby switchover should be completed within 1 second. That is, fast switchover is required on the bearer network.

Figure 7-19 Networking of VRRP fast switchover



Device	Interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF100	10.1.1.1/24
	XGE 0/0/2	VLANIF200	192.168.0.1/24
Switch B	XGE 0/0/1	VLANIF100	10.1.1.2/24
	XGE 0/0/2	VLANIF200	192.168.0.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Implement networking between the Switches.
2. Configure a BFD session on Switch A and Switch B to monitor Switch A and its downlink Switch A - Switch C - Switch D - Switch B.
3. Enable VRRP to track the BFD session on Switch B. When the BFD session becomes Down, the priority of Switch B increases by 40 and then the switchover is triggered.

NOTE

This example describes only the configurations on Switch A and Switch B.

Data Preparation

To complete the configuration, you need the following data:

- Local and remote discriminators of the BFD session
- ID and virtual IP address of the VRRP group
- Priorities of the S6700s in the VRRP group

Procedure

Step 1 Configure interworking between the Switches.

Assign IP addresses to all interfaces. # Configure OSPF between Switch A, Switch B, and Switch C.

For details, see **Figure 7-19**.

Step 2 Create a BFD session.

Create a BFD session on Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atob bind peer-ip 10.1.1.2 interface vlanif 200
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

Create a BFD session on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] bfd btoa bind peer-ip 10.1.1.1 interface vlanif 200
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

Run the **display bfd session** command on Switch A and Switch B, and you can see that the BFD session is Up. Take Switch A for example. The display is as follows:

```
[SwitchA] display bfd session all
--------------------------------------------------------------------------------
Local Remote PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
1     2      10.1.1.2  4     Up        Static      Vlanif200
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

Step 3 Configure VRRP fast switchover.

Create VRRP group 10 on Switch A and set the priority of Switch A in VRRP group 10 to 160 so that Switch A functions as the master in VRRP group 10.

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 10 virtual-ip 10.1.1.3
[SwitchA-Vlanif100] vrrp vrid 10 priority 160
[SwitchA-Vlanif100] quit
```

Create VRRP group 10 on Switch B and set the priority of Switch B in VRRP group 10 to 140 so that Switch B functions as the backup in VRRP group 10.

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 10 virtual-ip 10.1.1.3
[SwitchB-Vlanif100] vrrp vrid 10 priority 140
```

Configure VRRP to track the status of the BFD session on the backup device. If the BFD session becomes Down, the priority of Switch B increases by 40.

```
[SwitchB-Vlanif100] vrrp vrid 10 track bfd-session 2 increased 40
[SwitchB-Vlanif100] quit
```

Run the **display vrrp** command on Switch A or Switch B, and you can see that Switch A is the master and Switch B is the backup. You can also view the tracked BFD session and its status on Switch B.

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 10
    state : Master
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.1
    PriorityRun : 160
    PriorityConfig : 160
    MasterPriority : 160
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 10
    state : Backup
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.1
    PriorityRun : 140
    PriorityConfig : 140
    MasterPriority : 160
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Track BFD : 2  Priority increased : 40
```

```
    BFD-Session State : UP
    Config track link-bfd down-number : 0
```

Step 4 Verify the configuration.

Run the **shutdown** command on VLANIF 200 of Switch A to simulate a link fault.

```
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] shutdown
[SwitchA-Vlanif200] quit
```

On Switch B, VRRP fast switchover is performed after BFD fails.

```
%May 10 15:48:30 2008 SwitchB BFD/5/BFD:Slot=1;IO(1) BFD Session(Discr:2) FSM
Change To Down(Detect)
%May 10 15:48:30 2008 SwitchB VRRP/5/BfdWarning:
 Virtual Router 10 | BFD-SESSION 2 : BFD_STATE_UP --> BFD_STATE_DOWN
%May 10 15:48:30 2008 SwitchB VRRP/5/StateWarning:
 Vlanif100 | Virtual Router 10 :  BACKUP --> MASTER
```

Run the **display vrrp** command on Switch A, and you can see that the status of Switch A changes to Initialize.

```
[SwitchA] display vrrp
  Vlanif100 | Virtual Router 10
    state : Initialize
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.1
    PriorityRun : 160
    PriorityConfig : 160
    MasterPriority : 0
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

Run the **display vrrp** command on Switch B, and you can see that Switch B becomes the master, and the status of the BFD session changes to Down.

```
[SwitchB] display vrrp
  Vlanif100 | Virtual Router 10
    state : Master
    Virtual IP : 10.1.1.3
    Master IP : 10.1.1.2
    PriorityRun : 180
    PriorityConfig : 140
    MasterPriority : 180
    Preempt : YES   Delay Time : 0
    TimerRun : 1
    TimerConfig : 1
    Auth Type : NONE
    Virtual Mac :  0000-5e00-0110
    Check TTL : YES
    Config type : normal-vrrp
    Track BFD : 2  Priority increased : 40
    BFD-Session State : DOWN
    Config track link-bfd down-number : 0
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
  vlan batch 100 200
#
 bfd
#
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.3
 vrrp vrid 10 priority 160
#
interface Vlanif200
 ip address 192.168.0.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
bfd atob bind peer-ip 10.1.1.2 interface Vlanif 200
 discriminator local 1
 discriminator remote 2
 commit
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
  vlan batch 100 200
#
 bfd
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 10 virtual-ip 10.1.1.3
 vrrp vrid 10 priority 140
 vrrp vrid 10 track bfd-session 2 increased 40
#
interface Vlanif200
 ip address 192.168.0.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
bfd btoa bind peer-ip 10.1.1.1 interface Vlanif 200
 discriminator local 2
 discriminator remote 1
 commit
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
```

```
#
return
```

7.6.4 Example for Configuring VRRP6 on an Interface

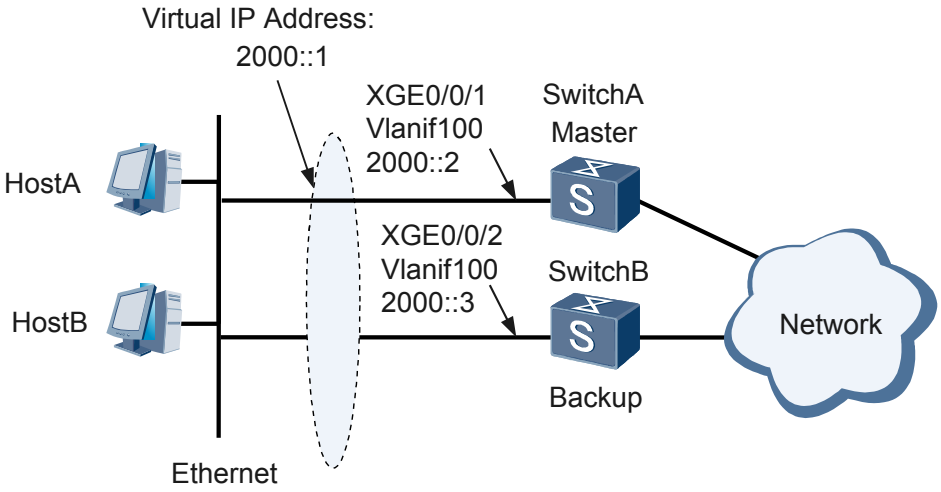
Networking Requirements

Switch A and Switch B elect a master device according to the configured priorities in a VRRP6 group.

Once the master device is determined in the group, only the master device responds to IPv6 messages. If the master device goes down, the backup device becomes the master device and the hosts in the private network can still communicate with external networks.

The configured virtual address can be same as the address of any physical interface of the Switch A or Switch B.

Figure 7-20 Networking of VRRP6



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IPv6 addresses for interfaces.
2. Configure virtual IPv6 addresses.

Data Preparation

To complete the configuration, you need the following data:

- VRRP6 group ID
- Priorities of the Switches in the VRRP6 group
- IPv6 addresses to be configured for interfaces
- Virtual IPv6 addresses to be configured for interfaces in the VRRP6 group

Procedure

Step 1 Enable IPv6 forwarding.

Configure SwitchA.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] ipv6
```

Configure SwitchB.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] ipv6
```

Step 2 Configure IPv6 addresses for interfaces.

Configure SwitchA.

```
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] interface xgigabitethernet0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 100
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ipv6 enable
[SwitchA-Vlanif100] ipv6 address 2000::2 64
```

Configure SwitchB.

```
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid pvid vlan 100
[SwitchB-XGigabitEthernet0/0/10] port hybrid untagged vlan 100
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ipv6 enable
[SwitchB-Vlanif100] ipv6 address 2000::3 64
```

Step 3 Configure virtual IPv6 addresses on interfaces in the VRRP6 group.

Configure SwitchA.

```
[SwitchA-Vlanif100] vrrp6 vrid 24 virtual-ip fe80::1 link-local
[SwitchA-Vlanif100] vrrp6 vrid 24 virtual-ip 2000::1
[SwitchA-Vlanif100] quit
```

Configure SwitchB.

```
[SwitchB-Vlanif100] vrrp6 vrid 24 virtual-ip fe80::1 link-local
[SwitchB-Vlanif100] vrrp6 vrid 24 virtual-ip 2000::1
```

Step 4 Set the priority of SwitchB to a value lower than the priority of SwitchA.

```
[SwitchB-Vlanif100] vrrp6 vrid 24 priority 25
[SwitchB-Vlanif100] quit
```

Step 5 Verify the configuration.

The following information shows that SwitchA is the master device, and SwitchB is the backup device.

```
[SwitchA] display vrrp6 interface vlanif 100
Vlanif100 | Virtual Router 24
    State : Master
    Virtual IP : FE80::1
```

```
                2000::1
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 25
    PriorityConfig : 25
    MasterPriority : 25
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0218
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
[SwitchB] display vrrp6 interface vlanif100
  Vlanif100 | Virtual Router 24
    State : Backup
    Virtual IP : FE80::1
                 2000::1
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 25
    PriorityConfig : 25
    MasterPriority : 25
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0218
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 100
#
ipv6
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::2/64
 vrrp6 vrid 24 virtual-ip FE80::1 link-local
 vrrp6 vrid 24 virtual-ip 2000::1
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 vlan batch 100
#
ipv6
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::3/64
 vrrp6 vrid 24 virtual-ip FE80::1 link-local
 vrrp6 vrid 24 virtual-ip 2000::1
 vrrp6 vrid 24 priority 25
#
```

```
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

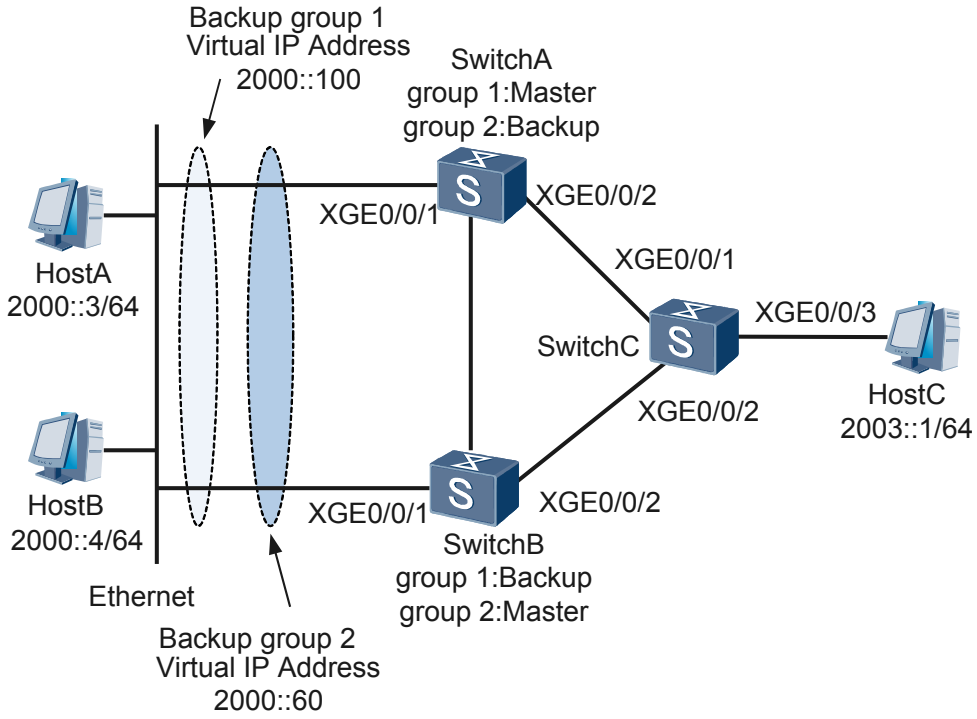
7.6.5 Example for Configuring VRRP6 in Load Balancing Mode

Networking Requirements

As shown in **Figure 7-21**,

- Switch A is the master device in VRRP group 1 and the backup device in VRRP group 2.
- Switch B is the master device in VRRP group 2 and the backup device in VRRP group 1.
- Host A on the LAN uses the virtual IPv6 address of VRRP group 1 as the gateway address, and Host B uses the virtual IPv6 address of VRRP group 2 as the gateway address. The two VRRP groups load balance traffic and back up each other.

Figure 7-21 Networking of VRRP in load balancing mode



Device	Interface	VLANIF interface	IP address
Switch A	XGE 0/0/1	VLANIF100	2000::1/64
	XGE 0/0/2	VLANIF200	2002::1/64
Switch B	XGE 0/0/1	VLANIF100	2000::2/64
	XGE 0/0/2	VLANIF400	2001::1/64
Switch C	XGE 0/0/1	VLANIF200	2002::2/64
	XGE 0/0/2	VLANIF400	2001::2/64

	XGE 0/0/3	VLANIF300	2003::2/64

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VRRP group 1 and VRRP group 2 on VLANIF 100 of Switch A. Ensure that Switch A is the master device in VRRP group 1 and the backup device in VRRP group 2.
2. Create VRRP group 1 and VRRP group 2 on VLANIF 100 of Switch B. Ensure that Switch B is the backup device in VRRP group 1 and the master device in VRRP group 1.

Data Preparation

To complete the configuration, you need the following data:

- IPv6 addresses of the interfaces
- IDs and virtual IPv6 addresses of the VRRP groups
- Priorities of the switches in each VRRP group

Procedure

Step 1 Configure IP addresses for the interfaces. The configuration procedure is not mentioned here.

Step 2 Configure OSPFv3 on Switch A, Switch B, and Switch C so that they can communicate with each other. The configuration procedure is not mentioned here.

Step 3 Configure the hosts.

Set the default gateway address of Host A to 2000::10, which is the virtual IPv6 address of VRRP group 1. Set the default gateway address of Host B to 2000::60, which is the virtual IPv6 address of VRRP group 2. Set the default gateway address of Host C to 2003::2.

Step 4 Configure VRRP6 groups.

Create VRRP group 1 and VRRP group 2 on VLANIF 100 of Switch A. Set the priority of Switch A in VRRP group 1 to 120 so that Switch A becomes the master device in VRRP group 1. Use the default priority of Switch A in VRRP group 2 so that Switch A becomes the backup device in VRRP group 2.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] interface vlanif100
[SwitchA-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[SwitchA-Vlanif100] vrrp6 vrid 1 virtual-ip 2000::100
[SwitchA-Vlanif100] vrrp6 vrid 1 priority 120
[SwitchA-Vlanif100] vrrp6 vrid 2 virtual-ip FE80::2 link-local
[SwitchA-Vlanif100] vrrp6 vrid 2 virtual-ip 2000::60
[SwitchA-Vlanif100] quit
```

Create VRRP group 1 and VRRP group 2 on VLANIF 100 of Switch B. Use the priority of Switch B in VRRP group 1 to 120 so that Switch B becomes the backup device in VRRP group 1. Set the priority of Switch B in VRRP group 2 to 120 so that Switch B becomes the master device in VRRP group 2.

```
<Quidway> system-view
[Quidway] sysname SwitchB
```

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[SwitchB-Vlanif100] vrrp6 vrid 1 virtual-ip 2000::100
[SwitchB-Vlanif100] vrrp6 vrid 2 virtual-ip FE80::2 link-local
[SwitchB-Vlanif100] vrrp6 vrid 2 virtual-ip 2000::60
[SwitchB-Vlanif100] vrrp6 vrid 2 priority 120
[SwitchB-Vlanif100] quit
```

Step 5 Verify the configuration.

After the preceding configuration is complete, Host A and Host C can ping Host B successfully. Run the **display vrrp6** command on Switch A, and you can find that VRRP group 1 and VRRP group 2 are created on Switch A. Switch A is the master device in VRRP group 1 and the backup device in VRRP group 2.

```
[SwitchA] display vrrp6
Vlanif100 | Virtual Router 1
    State : Master
    Virtual IP : FE80::1
                 2000::100
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0201
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0

  Vlanif100 | Virtual Router 2
    State : Backup
    Virtual IP : FE80::2
                 2000::60
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0202
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

Run the **display vrrp6** command on Switch B, and you can find that VRRP group 1 and VRRP group 2 are created on Switch B. Switch B is the backup device in VRRP group 1 and the master device in VRRP group 2.

```
[SwitchB] display vrrp6
Vlanif100 | Virtual Router 1
    State : Backup
    Virtual IP : FE80::1
                 2000::100
    Master IP : FE80::200:FF:FE00:24
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay time : 0
    TimerRun : 100
    TimerConfig : 100
    Virtual MAC :  0000-5e00-0201
    Check hop limit : YES
    Config type : normal-vrrp
    Config track link-bfd down-number : 0
```

```
Vlanif100 | Virtual Router 2
  State : Master
  Virtual IP : FE80::2
               2000::60
  Master IP : FE80::200:FF:FE00:24
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay time : 0
  TimerRun : 100
  TimerConfig : 100
  Virtual MAC :  0000-5e00-0202
  Check hop limit : YES
  Config type : normal-vrrp
  Config track link-bfd down-number : 0
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 100 200
#
 ipv6
#
ospfv3 1
 router-id 1.1.1.1
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::1/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local
 vrrp6 vrid 1 virtual-ip 2000::100
 vrrp6 vrid 1 priority 120
 vrrp6 vrid 2 virtual-ip FE80::2 link-local
 vrrp6 vrid 2 virtual-ip 2000::60
 ospfv3 1 area 0.0.0.0
 #
interface Vlanif200
 ipv6 enable
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid pvid untagged 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 200
 port hybrid pvid untagged 200
#

return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 100 400
#
 ipv6
#
ospfv3 1
 router-id 2.2.2.2
```

```
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2000::2/64
 vrrp6 vrid 1 virtual-ip FE80::1 link-local
 vrrp6 vrid 1 virtual-ip 2000::100
 vrrp6 vrid 2 virtual-ip FE80::2 link-local
 vrrp6 vrid 2 virtual-ip 2000::60
 vrrp6 vrid 2 priority 120
 ospfv3 1 area 0.0.0.0
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid pvid untagged 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 400
 port hybrid pvid untagged 400
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
 vlan batch 200 300 400
#
ipv6
#
ospfv3 1
 router-id 3.3.3.3
#
interface Vlanif200
 ipv6 enable
 ipv6 address 2002::2
 ospfv3 1 area 0.0.0.0
#
interface Vlanif300
 ipv6 enable
 ipv6 address 2003::2/64
 ospfv3 1 area 0.0.0.0
#
interface Vlanif400
 ipv6 enable
 ipv6 address 2001::2/64
 ospfv3 1 area 0.0.0.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 200
 port hybrid pvid untagged 200
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 300
 port hybrid pvid untagged 300
#
interface XGigabitEthernet0/0/3
 port hybrid pvid vlan 300
 port hybrid pvid untagged 300
#
return
```

7.7 MAC Swap Loopback Configuration

This chapter describes the working principle and configuration of MAC swap loopback.

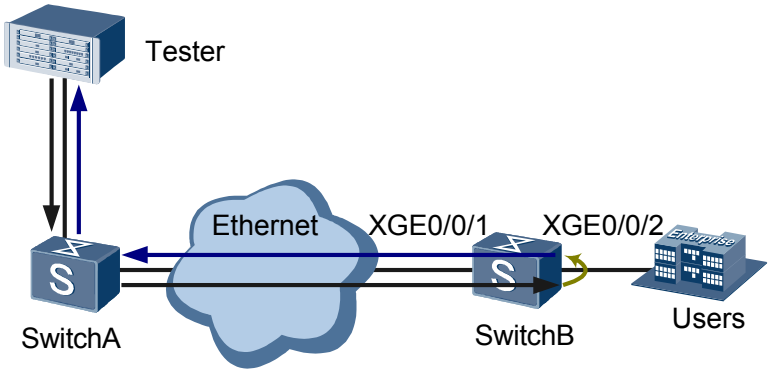
7.7.1 Example for Configuring Local MAC Swap Loopback

Networking Requirements

As shown in **Figure 7-22**, Switch B is an S6700. On Switch B, XGE 0/0/1 is connected to an Ethernet network, and XGE 0/0/2 is connected to users.

A local MAC swap loopback test needs to be performed on XGE 0/0/2. A tester sends Ethernet frames to Switch B. After the source and destination MAC addresses of the Ethernet frames are swapped on XGE 0/0/2, the Ethernet frames are sent back to the tester through XGE 0/0/1. The tester analyzes connectivity and performance of the Ethernet network and Switch B based on the received Ethernet frames.

Figure 7-22 Networking diagram of a local MAC swap loopback test



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN, configure XGE 0/0/1 as a trunk interface and XGE 0/0/2 as a hybrid interface, and add the interfaces to the VLAN.
2. Configure local MAC swap loopback on Switch B.
3. Enable the MAC swap loopback function on Switch B.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID: 100
- Source and destination MAC addresses of test Ethernet frames: 0018-2000-0085 and 0018-2000-0070

- Timeout period of the loopback test: 80s

Procedure

Step 1 Create VLAN 100, configure XGE 0/0/1 as trunk interface and XGE 0/0/2 as a hybrid interface, and add the interfaces to VLAN 100.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100
[SwitchB-XGigabitEthernet0/0/1] quit
[SwitchB] interface xgigabitethernet0/0/2
[SwitchB-XGigabitEthernet0/0/2] port hybrid pvid vlan 100
[SwitchB-XGigabitEthernet0/0/2] port hybrid untagged vlan 100
```

Step 2 Configure local MAC swap loopback on XGE 0/0/2 and specify XGE 0/0/1 as the outbound interface of loopback Ethernet frames. Enable the MAC swap loopback function.

```
[SwitchB-XGigabitEthernet0/0/2] loopback local swap-mac source-mac 0018-2000-0085
dest-mac 018-2000-0070 vlan 100 interface xgigabitethernet 0/0/1 timeout 80
[SwitchB-XGigabitEthernet0/0/2] loopback swap-mac start
[SwitchB-XGigabitEthernet0/0/2] quit
```

Step 3 Verify the configuration.

After completing the configuration, run the **display loopback swap-mac information** command to verify the configuration. If the configuration is correct, send Ethernet frames from the tester to test network performance.

```
[SwitchB] display loopback swap-mac information
  Loopback type             : local
  Loopback state            : running
  Loopback test time(s)     : 80
  Loopback interface        : XGigabitEthernet0/0/2
  Loopback output interface : XGigabitEthernet0/0/1
  Loopback source MAC       : 0018-2000-0085
  Loopback destination MAC  : 0018-2000-0070
  Loopback vlan             : 100
  Loopback inner vlan       : 0
  Loopback packets          : 0
  Drop packets              : 3
```

----End

Configuration Files

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 loopback local swap-mac source-mac 0018-2000-0085 dest-mac 0018-2000-0070
vlan
100 interface XGigabitEthernet0/0/1 timeout 80
```

```
#
return
```

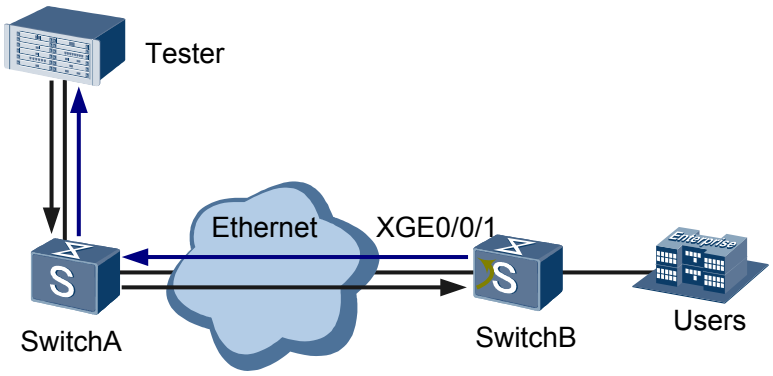
7.7.2 Example for Configuring Remote MAC Swap Loopback

Networking Requirements

As shown in **Figure 7-23**, Switch B is an S6700. XGE 0/0/1 of Switch B is connected to an Ethernet network.

A remote MAC swap loopback test needs to be performed on XGE 0/0/1. A tester sends Ethernet frames to Switch B. After the Ethernet frames are received on XGE 0/0/1, Switch B swaps their source and destination MAC addresses and sends them back to the tester from XGE 0/0/1. The tester analyzes connectivity and performance of the Ethernet network based on the received Ethernet frames.

Figure 7-23 Networking diagram of a remote MAC swap loopback test



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN, configure XGE 0/0/1 as a trunk interface, and add the interface to the VLAN.
2. Configure remote MAC swap loopback on Switch B.
3. Enable the MAC swap loopback function on Switch B.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID: 100
- Source and destination MAC addresses of test Ethernet frames: 0018-2000-0085 and 0018-2000-0070
- Timeout period of the loopback test: 80s

Procedure

Step 1 Create VLAN 100, configure XGE 0/0/1 as a trunk interface, and add XGE 0/0/1 to VLAN 100.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port link-type trunk
[SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 2 Configure remote MAC swap loopback and enable the MAC swap loopback function on XGE 0/0/1.

```
[SwitchB-XGigabitEthernet0/0/1] loopback remote swap-mac source-mac 0018-2000-0085
dest-mac 018-2000-0070 vlan 100 timeout 80
[SwitchB-XGigabitEthernet0/0/1] loopback swap-mac start
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 3 Verify the configuration.

After completing the configuration, run the **display loopback swap-mac information** command to verify the configuration. If the configuration is correct, send Ethernet frames from the tester to test network performance.

```
[SwitchB] display loopback swap-mac information
  Loopback type             : remote
  Loopback state            : running
  Loopback test time(s)     : 80
  Loopback interface        : XGigabitEthernet0/0/1
  Loopback output interface : XGigabitEthernet0/0/1
  Loopback source MAC       : 0018-2000-0085
  Loopback destination MAC  : 0018-2000-0070
  Loopback vlan             : 100
  Loopback inner vlan       : 0
  Loopback packets          : 0
```

----End

Configuration Files

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 100
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 loopback remote swap-mac source-mac 0018-2000-0085 dest-mac 0018-2000-0070
vlan
 100 timeout 80
#
return
```

8 Configuration Guide - Device Management

About This Chapter

This document describes procedures and provides examples for configuring the Device Management features of the S6700.

8.1 NAP Configuration

This chapter describes how to configure the Neighbor Access Protocol (NAP) on the S6700.

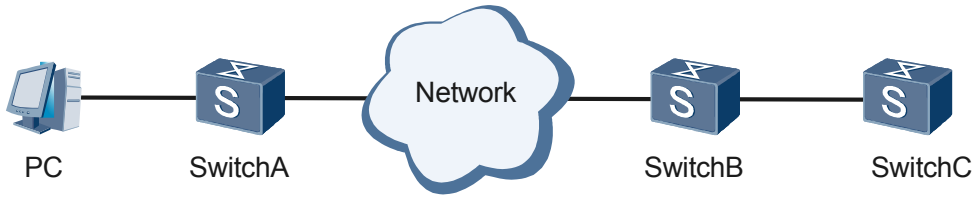
8.1.1 Example for Configuring NAP-based Remote Deployment in Static Mode

In this example, the temporary neighbor relationship is set up between the switch and the device with the empty configuration and IP addresses are assigned to the switch and the device to implement remote deployment in manual mode.

Networking Requirements

As shown in **Figure 8-1**, the user needs to perform a remote login to Switch B from Switch A. Switch B is the master device, and temporary neighbor relationship is to be set up between Switch B and Switch C having an empty configuration. Switch B and Switch C need to be directly connected via a single hop. Both the interfaces connecting Switch B and Switch C should be in the Up state, and should support NAP.

Figure 8-1 Networking diagram of NAP-based remote deployment



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a NAP master interface on Switch B.
2. Configure an IP address for establishing a NAP connection on Switch B.
3. Use NAP to log in to Switch C from Switch B by means of Telnet.

Data Preparation

To complete the configuration, you need the following data:

- Two primary IP addresses. The two IP addresses are primary IP addresses for the master interface and the slave interface respectively, and should be on the same network segment.
- Two secondary IP addresses. The two IP addresses are secondary IP addresses for the master interface and the slave interface respectively, and should be on the same network segment.

Procedure

Step 1 Configure a NAP master interface on Switch B

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] nap port master
```

Step 2 Configure an IP address for establishing a NAP connection on Switch B

```
[SwitchB-XGigabitEthernet0/0/1] nap local-ip 12.12.12.5 sub-ip 12.12.12.9 peer-ip
12.12.12.6 sub-ip 12.12.12.10 30
Are you sure to continue?[Y/N] y
```

After the preceding configuration is complete, run the **display nap status** command on Switch B. You can view that NAP has been enabled on Switch B. Then, run the **display nap interface** command. You can view that the primary and secondary IP addresses have been assigned to the master and slave interfaces. For example:

```
[SwitchB-XGigabitEthernet0/0/1] display nap status
Slave port status         : Enable
 Nap ip-pool/Mask          : 10.167.253.0/24
[SwitchB-XGigabitEthernet0/0/1] display nap interface
------------------------------------------------------
 NAP master port list
 Port count           : 1
------------------------------------------------------
 Port property                          : Master
 Current status                         : IP-ASSIGNED
 Local port                             : XGigabitEthernet0/0/1
 Peer port                              : XGigabitEthernet0/0/1
 Local primary ip                       : 12.12.12.5
 Peer primary ip                        : 12.12.12.6
 Local secondary ip                     : 12.12.12.9
 Peer secondary ip                      : 12.12.12.10
 Hello time                             : 3s
 Linked time                            : 00:02:33
------------------------------------------------------
```

Step 3 Log in to the slave device from the master device.

Configure Switch B.

```
[SwitchB-XGigabitEthernet0/0/1] nap login neighbor
Trying 12.12.12.10 ...
Press CTRL+K to abort
Connected to 12.12.12.10 ...

Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
```

Step 4 Disable NAP on the slave device.

Configure Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] undo nap slave enable
```

----End

Configuration Files

None

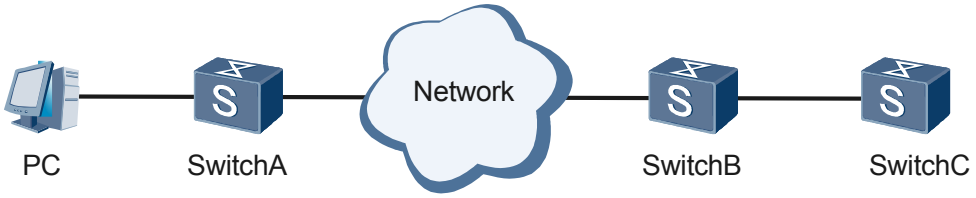
8.1.2 Example for Configuring NAP-based Remote Deployment in Automatic Mode

In this example, the temporary neighbor relationship is set up between a switch and another switch that has the empty configuration to implement remote deployment in automatic mode.

Networking Requirements

As shown in **Figure 8-2**, the user needs to perform a remote login to Switch B from Switch A. Switch B is the master device, and temporary neighbor relationship is to be set up between Switch B and Switch C having an empty configuration. Switch B and Switch C need to be directly connected via a single hop. Both the interfaces connecting Switch B and Switch C should be in the Up state, and should support NAP.

Figure 8-2 Networking diagram of NAP-based remote deployment



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a primary IP address and a secondary IP address on Switch B.
2. Configure a NAP master interface on Switch B.
3. Telnet to Switch C from Switch B by means of NAP.

Data Preparation

None

Procedure

Step 1 Configuring the NAP master interface

Do as follows on Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] interface xgigabitethernet0/0/1
[SwitchB-XGigabitEthernet0/0/1] nap port master
```

Step 2 Logging in to the slave device from the master device.

Do as follows on Switch B.

```
[SwitchB-XGigabitEthernet0/0/1] nap login neighbor
Trying 10.167.253.10 ...
Press CTRL+K to abort
Connected to 10.167.253.10 ...
```

```
Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
```

Step 3 Shutting down NAP on the slave device.

Do as follows on Switch C.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] undo nap slave enable
```

----End

Configuration Files

None

8.2 Stacking

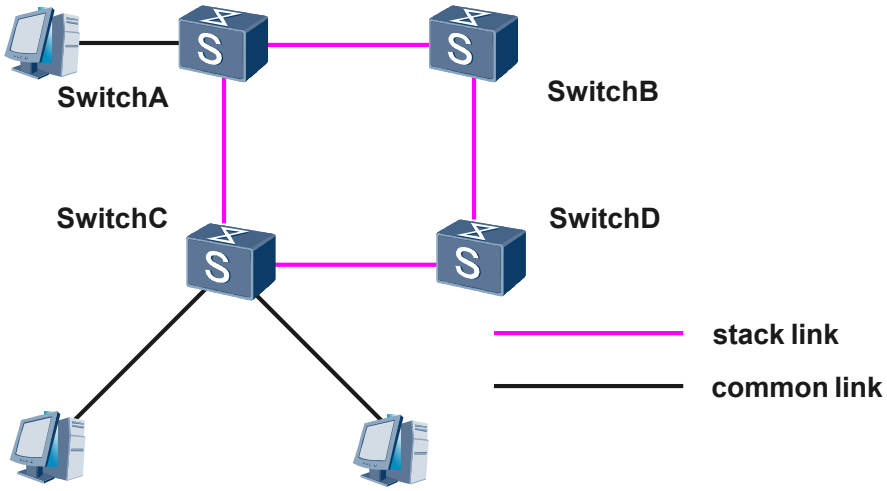
This chapter describes the basic concepts and configuration methods of the stacking function.

8.2.1 Example for Configuring a Stack in a Ring Topology

Networking Requirements

As shown in **Figure 8-3**, Switch A, Switch B, Switch C, and Switch D form a stack in a ring topology. The stack system is automatically created. Switch A functions as the master switch, whereas Switch B functions as a standby switch. After the active/standby switchover, the MAC address of the stack system is immediately switched. To avoid updating MAC addresses of the stack system frequently and wasting system resources, set the MAC address switchover time of the stack system to 1 minute after the active/standby switchover.

Figure 8-3 Networking of a stack in a ring topology



Configuration Roadmap

The configuration roadmap is as follows:

- Configure the MAC address switchover time of the stack system on the master switch.

Data Preparation

To complete the configuration, you need the following data:

- Service interfaces that need to be configured as stack interfaces on the master switch
- Member interfaces to be added to the stack interfaces on the master switch
- MAC address switchover time of the stack system

Configuration Procedure

1. Enable the stack interface function on XGE0/0/1 through XGE0/0/4 as stack interfaces on SwitchA.

```
<SwitchA> system view
[SwitchA] stack port interface XGigabitEthernet 0/0/1 to 0/0/4 enable
```

2. Configure interfaces XGE0/0/1 through XGE0/0/4 as stack interfaces on SwitchA.

```
[SwitchA] interface stack-port 0/1
[Quidway-stack-port0/1] port member-group interface XGigabitEthernet 0/0/1
[Quidway-stack-port0/1] quit
[SwitchA] interface stack-port 0/2
[Quidway-stack-port0/2] port member-group interface XGigabitEthernet 0/0/2
```

3. # Configure the MAC address switchover time of the stack system on Switch A.

```
<SwitchA> system-view
[SwitchA] stack timer mac-address switch-delay 1
```

Run the **display stack** command on Switch A to check basic information about a stack.

```
<SwitchA> display stack
Stack topology type: Ring
Stack system MAC: 0018-82b1-6eb8
MAC switch delay time: 1 min
Stack reserved vlanid : 4093
slot#     role        Mac address      Priority   Device type
------    ----        --------------   ------     -------
    0     Slave       0018-82d2-2e85   100        S6700-48-EI
    1     Slave       0018-82c6-1f44   100        S6700-48-EI
    3     Standby     0018-82c6-1f4c   100        S6700-48-EI
    4     Master      0018-82b1-6eb8   100        S6700-48-EI
```

Configuration Files

None.

8.3 Monitoring the Device Through the Information Center

This chapter describes the basics of the information center, introduces the procedure for managing the information center and monitoring the device, and provides configuration examples.

8.3.1 Example for Configuring the Information Center

Networking Requirements

Figure 8-4 Networking of sending logs to the log host

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the information center.
2. Configure the information channel to ensure that the S6700 can correctly send logs to the log host. Disable the sending of the traps and debugging information to the log host.
3. Configure the log host.

Data Preparation

To complete the configuration, you need the following data:

- The IP address of the log host is specified as 1.0.0.1/8.

Configuration Procedure

NOTE

In the example, only the commands related to monitoring are listed. For details on configuring the log host, see the help files on the log host.

1. Enable the information center.

   # Enable the information center. By default, the information center on the S6700 is enabled.

   ```
   <Quidway> system-view
   [Quidway] info-center enable
   Info:Information center is enabled
   ```

2. Configure the information channel.

   # Send logs of severity levels 0 to 7 from all modules on the S6700 through the channel to the log host. Disable the sending of the debugging information and traps through the channel to the log host.

   ```
   [Quidway] info-center source default channel loghost log level debugging state
   on trap state off debug state off
   ```

   # Verify the configuration.

   ```
   [Quidway] display channel loghost
   channel number:2, channel name:loghost
   MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
   ffff0000 default  Y      debugging     N      debugging     N      debugging
   ```

3. Configure the log host.

   # Set the IP address of the log host to 1.0.0.1.

```
[Quidway] info-center loghost 1.0.0.1
```

   # Set VLANIF 10 as the interface for sending information to the log host on the S6700.

```
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface xgigabitethernet0/0/1
[Quidway-XGigabitEthernet0/0/1] port link-type hybrid
[Quidway-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-XGigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-vlanif10] ip address 2.0.0.1 255.0.0.0
[Quidway-vlanif10] quit
[Quidway] info-center loghost source vlanif 10
```

   # Verify the configuration.

```
[Quidway] display info-center
Information Center:enabled
Log host:
         the interface name of the source address:vlanif 10
         1.0.0.1, channel number 2, channel name loghost,
                                    language English , host facility local7
Console:
         channel number : 0, channel name : console
Monitor:
         channel number : 1, channel name : monitor
SNMP Agent:
         channel number : 5, channel name : snmpagent
Log buffer:
         enabled,max buffer size 1024, current buffer size 512,
current messages 440, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 0
Trap buffer:
         enabled,max buffer size 1024, current buffer size 256,
current messages 1, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
Information timestamp setting:
         log - date, trap - date, debug - boot

 Sent messages = 499, Received messages = 499

 IO Reg messages = 0 IO Sent messages = 0
```

4. Enable the terminal display of the console.

   # Enable the terminal display of the console. Enable the corresponding terminal display to check the information type as required.

```
[Quidway] info-center console channel 0
[Quidway] quit
<Quidway> terminal monitor
Info:Current terminal monitor is on
<Quidway> terminal logging
Info:Current terminal logging is on
```

Configuration Files

```
#
 info-center source default channel 2 log level debugging state on trap state off
debug state off
 info-center loghost source vlanif 10
 info-center loghost 1.0.0.1

#
#
 vlan batch 10
#
```

```
interface vlanif10
 ip address 2.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 10
#
return
```

8.4 Mirroring

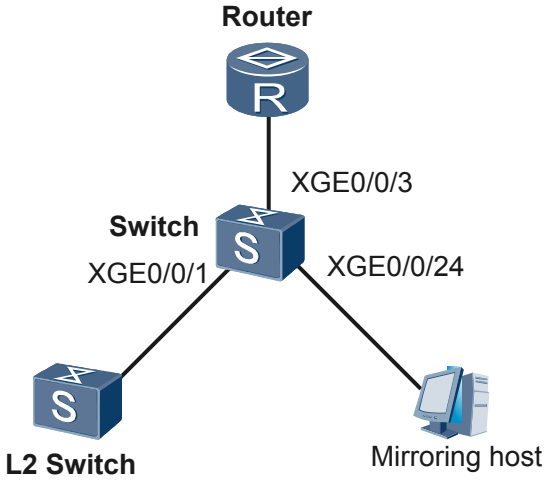
The mirroring function is used to monitor packets that meet certain requirements.

8.4.1 Example for Configuring Local Port Mirroring

Networking Requirements

As shown in **Figure 8-5**, a Layer 2 (L2) switch is connected to XGigabitEthernet 0/0/1 on the Switch, and the incoming traffic on XGigabitEthernet 0/0/1 needs to be monitored. In this case, you can configure local port mirroring with XGigabitEthernet 0/0/1 as a mirrored port and XGigabitEthernet 0/0/24 as an observing port.

Figure 8-5 Networking diagram of local port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure XGigabitEthernet 0/0/24 as an observing port.
2. Configure XGigabitEthernet 0/0/1 as a mirrored port.

Data Preparation

None.

Configuration Procedure

1. Create a VLAN on the Switch and add interfaces to the VLAN in trunk mode.

   # Add XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/3 to a same VLAN in trunk mode. The following takes the configuration of XGigabitEthernet 0/0/1 as an example. The configuration of XGigabitEthernet 0/0/3 is the same as the configuration of XGigabitEthernet 0/0/1 and is not mentioned here.

   ```
   <Switch> system-view
   [Switch] vlan 1
   [Switch-vlan1] quit
   [Switch] interface xgigabitethernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 1
   [Switch-XGigabitEthernet0/0/1] quit
   ```

2. Configure an observing port.

   # Set XGigabitEthernet 0/0/24 as the observing port.

   ```
   <Switch> system-view
   [Switch] observing-port 1 interface XGigabitEthernet 0/0/24
   ```

3. Configure a mirrored port.

   # Set XGigabitEthernet 0/0/1 as a mirrored port.

   ```
   [Switch] interface xgigabitethernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
   [Switch-XGigabitEthernet0/0/1] quit
   ```

4. Verify the configuration.

   # Run the **display port-mirroring** command. You can check the configurations on the observing port and mirrored port.

   ```
   [Switch] display port-mirroring
    Observe index 1 is set to interface XGigabitEthernet0/0/24
      Observe Type: Local
    Interface XGigabitEthernet0/0/1
     Mirrored to: Observe index 1
       Direction: inbound
    Observe index 2 is not set to any interface
    Observe index 3 is not set to any interface
    Observe index 4 is not set to any interface
   ```

Configuration Files

Configuration file of the Switch

```
#
vlan batch 1
#
 sysname Switch
#
 observing-port 1 interface XGigabitEthernet0/0/24
#
interface XGigabitEthernet0/0/1
 port trunk allow-pass vlan 1
 port-mirroring to observe-port 1 inbound
#
interface XGigabitEthernet0/0/3
 port trunk allow-pass vlan 1
#
return
```

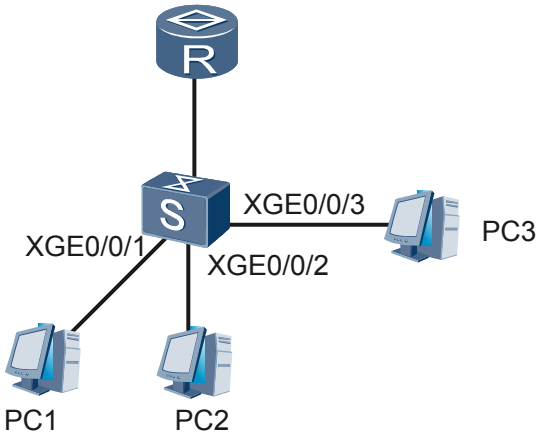
8.4.2 Example for Configuring Local VLAN Mirroring

Networking Requirements

As shown in **Figure 8-6**, XGigabitEthernet0/0/1 is connected to PC1; XGigabitEthernet0/0/2 is connected to PC2. PC1 and PC2 belong to VLAN 10. Now, incoming traffic of all active interfaces in VLAN 10 needs to be monitored. In this case, you can configure local VLAN mirroring.

XGigabitEthernet0/0/3 serves as an observing port.

Figure 8-6 Networking diagram of local VLAN mapping



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure XGigabitEthernet0/0/3 as an observing port.
2. Configure VLAN 10 as a mirrored VLAN.

Data Preparation

None.

Configuration Procedure

1. Add XGigabitEthernet0/0/1 and XGigabitEthernet0/0/2 to VLAN 10 as access interfaces.

   # Add XGigabitEthernet0/0/1 to VLAN 10 as an access interface.

   ```
   <Switch> system-view
   [Switch] interface xgigabitethernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] port link-type access
   [Switch-XGigabitEthernet0/0/1] port default vlan 10
   [Switch-XGigabitEthernet0/0/1] quit
   ```

   Add XGigabitEthernet0/0/2 to VLAN 10 as an access interface in the same way.

2. Configure an observing port.

   # Set XGigabitEthernet0/0/3 as an observing port.

   ```
   [Switch] observing-port 1 interface xgigabitethernet 0/0/3
   ```

3. Configure a mirrored VLAN.

   # Set VLAN 10 as a mirrored VLAN.

```
[Switch] VLAN 10
[Switch-VLAN10] mirroring to observe-port 1 inbound
[Switch-VLAN10] quit
```

4. Verify the configuration.

   # Run the **display port-mirroring** command. You can view the configuration of the observing port.

```
[Switch] display port-mirroring
 Observe index 1 is set to interface XGigabitEthernet0/0/3
   Observe Type: Local
 Observe index 2 is not set to any interface
 Observe index 3 is not set to any interface
 Observe index 4 is not set to any interface
```

Configuration Files

Configuration file of the Switch

```
#
sysname Switch
#
 vlan batch 10
#
 observe-port 1 interface XGigabitEthernet0/0/3
#
vlan 10
 mirroring to observe-port 1 inbound
#
interface XGigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#

#
return
```

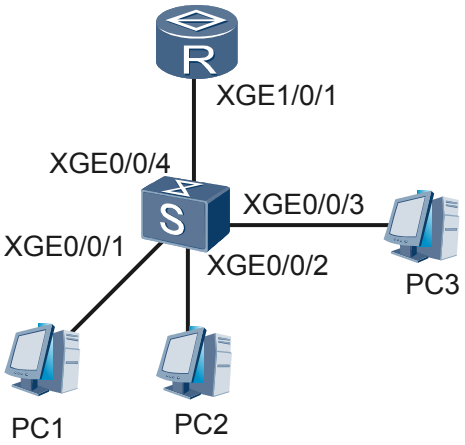
8.4.3 Example for Configuring MAC Address-based Local Mirroring

Networking Requirements

As shown in **Figure 8-7**, XGigabitEthernet 0/0/1 is connected to PC1; XGigabitEthernet 0/0/2 is connected to PC2; XGigabitEthernet 0/0/4 is connected to a router. XGigabitEthernet 0/0/1, XGigabitEthernet 0/0/2, and XGigabitEthernet 0/0/4 belong to VLAN 10. Now, incoming traffic with the source or destination MAC as the MAC address of XGigabitEthernet 1/0/1 on the router in VLAN 10 needs to be monitored. In this case, you can configure local MAC address mirroring on the Switch.

XGigabitEthernet 0/0/3 serves as an observing port. The MAC address of XGigabitEthernet 1/0/1 is 0001-0001-0001.

Figure 8-7 Networking diagram of local MAC address mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Set XGigabitEthernet 0/0/3 as an observing port.
2. Configure local MAC address mirroring in the view of VLAN 10.

Data Preparation

None.

Configuration Procedure

1. Configure VLAN 10 and then add XGigabitEthernet 0/0/1, XGigabitEthernet 0/0/2, and XGigabitEthernet 0/0/4 to VLAN 10. The configuration procedure is not mentioned here.
2. # Set XGigabitEthernet 0/0/3 as an observing port.

   ```
   <Switch> system-view
   [Switch] observing-port 1 interface XGigabitEthernet 0/0/3
   ```

3. Configure a mirroring MAC.

   # Configure local MAC address mirroring in the view of VLAN 10.

   ```
   [Switch] VLAN 10
   [Switch-VLAN10] mac-mirroring 0001-0001-0001 to observe-port 1 inbound
   [Switch-VLAN10] quit
   ```

4. Verify the configuration.

   # Run the **display port-mirroring** command. You can view the configuration of the observing port.

   ```
   [Switch] display port-mirroring
    Observe index 1 is set to interface XGigabitEthernet0/0/3
      Observe Type: Local
    Observe index 2 is not set to any interface
    Observe index 3 is not set to any interface
    Observe index 4 is not set to any interface
   ```

Configuration Files

Configuration file of the Switch

```
#
sysname Switch
#
 vlan batch 10
#
 observing-port 1 interface XGigabitEthernet0/0/3
#
vlan 10
 mac-mirroring 0001-0001-0001 to observe-port 1 inbound
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
#

#
return
```

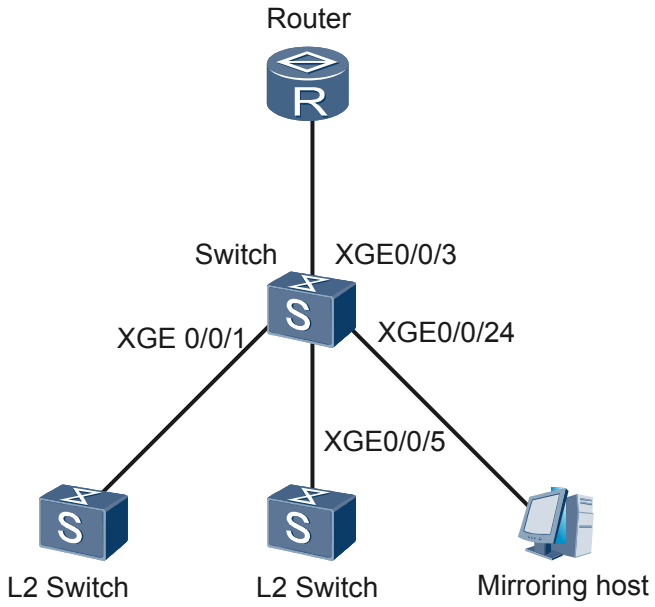
8.4.4 Example for Configuring Local Flow Mirroring

Networking Requirements

As is shown in **Figure 8-8**, the Switch is connected to two L2 switches through XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/5. Packets with the same attributes received by XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/5 and transmitted from XGigabitEthernet 0/0/3 need to be monitored. In this example, packets with the 802.1p priority as 6 need to be monitored.

XGigabitEthernet 0/0/24 is configured as an observing port.

Figure 8-8 Networking diagram of local flow mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure XGigabitEthernet 0/0/24 as an observing port.
2. Create a traffic classifier and set the traffic classification rule that only the packets with the 802.1p priority as 6 can be matched.
3. Create a traffic behavior and configure flow mirroring in the traffic behavior.
4. Create a traffic policy and bind the traffic classifier to the traffic behavior.
5. Apply the traffic policy to XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/5.
6. Create a VLAN on the Switch. Add XGigabitEthernet 0/0/1, XGigabitEthernet 0/0/3, and XGigabitEthernet 0/0/5 to the same VLAN in trunk mode.

Data Preparation

To complete the configuration, you need the following data:

- Name of the traffic classifier: c1
- Name of the traffic behavior: b1
- Name of the traffic policy: p1
- ID of the VLAN created on the Switch: 1

Configuration Procedure

1. Create a VLAN on the Switch and add interfaces to the VLAN in trunk mode.

   # Add XGigabitEthernet 0/0/1, XGigabitEthernet 0/0/3, and XGigabitEthernet 0/0/5 to the same VLAN in trunk mode. The following takes the configuration of XGigabitEthernet 0/0/1 as an example. The configurations of XGigabitEthernet 0/0/3 and

XGigabitEthernet 0/0/5 are the same as the configuration of XGigabitEthernet 0/0/1 and are not mentioned here.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface xgigabitethernet 0/0/1
[Switch-XGigabitEthernet0/0/1] port link-type trunk
[Switch-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-XGigabitEthernet0/0/1] quit
```

2. Configure an observing port.

   # Configure XGigabitEthernet 0/0/24 as the observing port.

   ```
   [Switch] observe-port 1 interface xgigabitethernet 0/0/24
   ```

3. # Create a traffic classifier.

   # Create traffic classifier **c1** and set the traffic classification rule that only the packets with the 802.1p priority as 6 can be matched.

   ```
   [Switch] traffic classifier c1
   [Switch-classifier-c1] if-match 8021p 6
   [Switch-classifier-c1] quit
   ```

4. # Create a traffic behavior.

   # Create traffic behavior **b1** and configure flow mirroring in the traffic behavior.

   ```
   [Switch] traffic behavior b1
   [Switch-behavior-b1] mirroring to observe-port 1
   [Switch-behavior-b1] quit
   ```

5. Create a traffic policy.

   # Create a traffic policy and bind traffic classifier **c1** to traffic behavior **b1**.

   ```
   [Switch] traffic policy p1
   [Switch-trafficpolicy-p1] classifier c1 behavior b1
   [Switch-trafficpolicy-p1] quit
   ```

6. Apply the traffic policy and enable the interface to trust the 802.1p priority of packets.

   # Apply traffic policy **p1** to XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/5, and enable XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/5 to trust the 802.1p priority of packets.

   ```
   [Switch] interface xgigabitethernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] traffic-policy p1 inbound
   [Switch-XGigabitEthernet0/0/1] trust 8021p inner
   [Switch-XGigabitEthernet0/0/1] quit
   [Switch]interface xgigabitethernet 0/0/5
   [Switch-XGigabitEthernet0/0/5] traffic-policy p1 inbound
   [Switch-XGigabitEthernet0/0/5] trust 8021p inner
   [Switch-XGigabitEthernet0/0/5] quit
   ```

7. Verify the configuration.

   # Run the **display port-mirroring** command. You can check the observing port.

   ```
   [Switch] display port-mirroring
   ```

   # Run the **display traffic policy interface** command. You can check the traffic policy applied to XGigabitEthernet 0/0/1 and XGigabitEthernet 0/0/5.

   ```
   [Switch] display traffic policy interface
     Interface: XGigabitEthernet0/0/1
     Direction: Inbound
     Policy: p1
      Classifier: c1
   Rule(s) :
           if-match 8021p 6
       Behavior: b1
           Mirroring to observe-port 1

     Interface: XGigabitEthernet0/0/5
     Direction: Inbound
   ```

```
  Policy: p1
   Classifier: c1
Rule(s) :
        if-match 8021p 6
     Behavior: b1
         Mirroring to observe-port 1
```

Configuration Files

Configuration file of the Switch

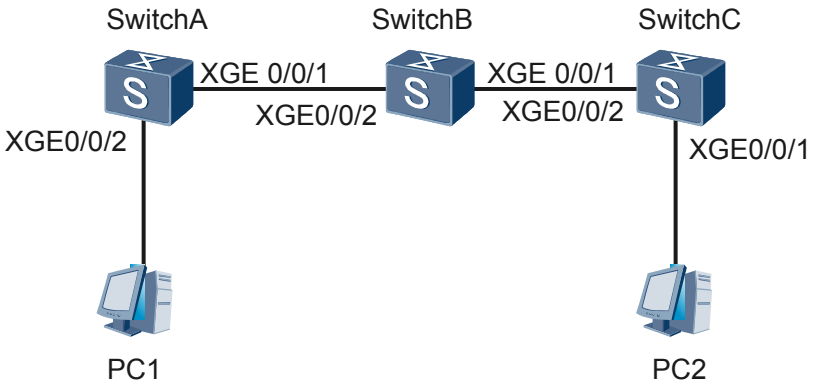
```
#
sysname Switch
#
vlan batch 10
#
 observe-port 1 interface XGigabitEthernet0/0/24
#
traffic classifier c1
 if-match 8021p 6
#
traffic behavior b1
 mirroring to observe-port 1
#
traffic policy p1
 classifier c1 behavior b1
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy p1 inbound
 trust 8021p inner
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface XGigabitEthernet0/0/5
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy p1 inbound
 trust 8021p inner
#
interface XGigabitEthernet0/0/24
#
return
```

8.4.5 Example for Configuring Remote Port Mirroring

Networking Requirements

As shown in **Figure 8-9**, Switch A is connected to PC1; Switch C is connected to PC2. Now, incoming traffic of XGigabitEthernet0/0/2 on Switch A needs to be monitored on PC2. In this case, you can configure remote port mirroring on Switch A.

Figure 8-9 Networking diagram of remote port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

- Configure XGigabitEthernet0/0/1 of Switch A as an observing port and specify the RSPAN VLAN.
- Configure XGigabitEthernet0/0/2 of Switch A as a mirrored port.
- Configure XGigabitEthernet0/0/1 of Switch C as an observing port.

Data Preparation

To complete the configuration, you need the following data:

- Index of the observing port on Switch A: 1
- ID of the RSPAN VLAN on Switch A, Switch B, and Switch C: 2
- Index of the observing port on Switch C: 1

Configuration Procedure

1. Configure Switch A.

   # Configure the RSPAN VLAN.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] quit
   ```

   # Configure XGigabitEthernet0/0/1 of Switch A as an observing port and specify the RSPAN VLAN.

   ```
   [SwitchA] observe-port 1 interface xgigabitethernet 0/0/1 vlan 2
   ```

   # Add XGigabitEthernet0/0/1 to the RSPAN VLAN as a trunk interface.

   ```
   [SwitchA] interface xgigabitethernet 0/0/1
   [SwitchA-XGigabitEthernet0/0/1] port link-type trunk
   [SwitchA-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2
   [SwitchA-XGigabitEthernet0/0/1] quit
   ```

   # Configure remote port mirroring for incoming traffic on XGigabitEthernet0/0/2.

   ```
   [SwitchA] interface xgigabitethernet 0/0/2
   [SwitchA-XGigabitEthernet0/0/2] port-mirroring to observe-port 1 inbound
   [SwitchA-XGigabitEthernet0/0/2] quit
   ```

2. Configure Switch B.

   # Create the RSPAN VLAN.

   ```
   <SwitchB> system-view
   [SwitchB] vlan 2
   [SwitchB-vlan2] quit
   ```

   # Add XGigabitEthernet0/0/1 and XGigabitEthernet0/0/2 to the RSPAN VLAN as trunk interfaces.

   ```
   [SwitchB] interface xgigabitethernet 0/0/1
   [SwitchB-XGigabitEthernet0/0/1] port link-type trunk
   [SwitchB-XGigabitEthernet0/0/1] port trunk allow-pass vlan 2
   [SwitchB-XGigabitEthernet0/0/1] quit
   [SwitchB] interface xgigabitethernet 0/0/2
   [SwitchB-XGigabitEthernet0/0/2] port link-type trunk
   [SwitchB-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2
   [SwitchB-XGigabitEthernet0/0/2] quit
   ```

3. Configure Switch C.

   # Create the RSPAN VLAN.

   ```
   <SwitchC> system-view
   [SwitchC] vlan 2
   [SwitchC-vlan2] quit
   ```

   # Add XGE 0/0/2 to the RSPAN VLAN as a trunk interface.

   ```
   [SwitchC] interface xgigabitethernet 0/0/2
   [SwitchC-XGigabitEthernet0/0/2] port link-type trunk
   [SwitchC-XGigabitEthernet0/0/2] port trunk allow-pass vlan 2
   [SwitchC-XGigabitEthernet0/0/2] quit
   ```

   # Configure XGE 0/0/1 as a hybrid interface and configure it to allow packets of the RSPAN VLAN to pass.

   ```
   [SwitchC] interface xgigabitethernet 0/0/1
   [SwitchC-XGigabitEthernet0/0/1] port hybrid untagged vlan 2
   [SwitchC-XGigabitEthernet0/0/1] quit
   ```

Configuration Files

Configuration file of Switch A

```
#
sysname SwitchA
#
vlan 2
#
 observe-port 1 interface XGigabitEthernet0/0/1 vlan 2
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface XGigabitEthernet0/0/2
 port-mirroring to observe-port 1 inbound
#

#
return
```

Configuration file of Switch B

```
sysname SwitchB
#
vlan 2
#
```

```
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#

#
return
```

Configuration file of Switch C

```
#
sysname SwitchC
#
vlan 2
#
interface XGigabitEthernet0/0/1
 port hybrid untagged vlan 2
#
interface XGigabitEthernet0/0/2
  port link-type trunk
 port trunk allow-pass vlan 2
#

#
return
```

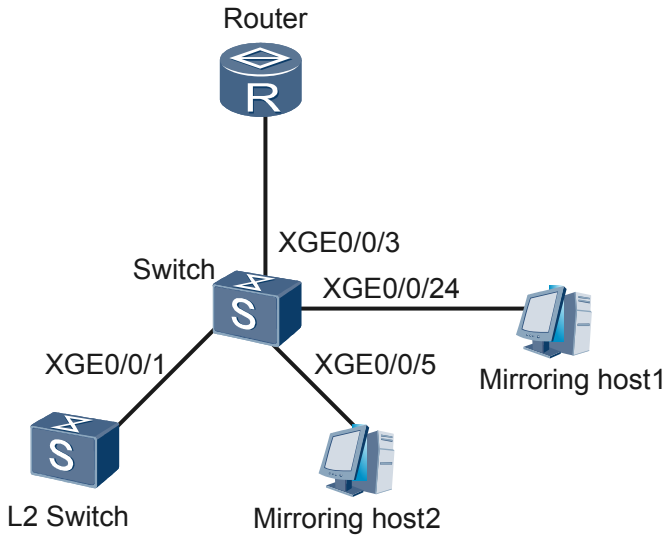
8.4.6 Example for Changing an Observing Port

Networking Requirements

As shown in **Figure 8-10**,XGigabitEthernet 0/0/1 on the Switch is connected to an L2 switch; XGigabitEthernet 0/0/24 is connected to host 1; XGigabitEthernet 0/0/5 is connected to host 2. To monitor incoming traffic on XGigabitEthernet 0/0/1, port mirroring is configured on the Switch. Configure XGigabitEthernet 0/0/1 as a mirrored port, and XGigabitEthernet 0/0/24 connected to host 1 as an observing port. Enable host 1 to receive incoming traffic from XGigabitEthernet 0/0/1.

At present, host 2 needs to receive incoming traffic from XGigabitEthernet 0/0/1. Therefore, the observing port needs to switch from XGigabitEthernet 0/0/24 to XGigabitEthernet 0/0/5.

Figure 8-10 Networking for changing the observing port



Configuration Roadmap

The configuration roadmap is as follows:

1. Delete the mirrored port XGigabitEthernet 0/0/1.
2. Set XGigabitEthernet 0/0/5 instead of XGigabitEthernet 0/0/24 as the observing port.
3. Reset XGigabitEthernet 0/0/1 as a mirrored port.

Data Preparation

To complete the configuration, you need the following data:

- Type and number of the new observing port, that is, XGigabitEthernet 0/0/5

Configuration Procedure

1. Check the configurations on the current observing port and mirrored port.

   # Run the **display port-mirroring** command to check the configurations on the current observing port and mirrored port.

   ```
   <Switch> display port-mirroring
     Port-
   mirror:
   ------------------------------------------------------------
     Mirror-port              Direction     Observe-port
   ------------------------------------------------------------
     XGigabitEthernet0/0/1     Inbound
   XGigabitEthernet0/0/24
   ```

2. Delete the mirrored port.

   # Delete the mirrored port XGigabitEthernet 0/0/1.

   ```
   <Switch> system-view
   [Switch] interface XGigabitEthernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] undo port-mirroring inbound
   ```

3. Delete the observing port.

Delete the observing port XGigabitEthernet 0/0/24.

```
<Switch> system-view
[Switch] undo observe-port 1
```

4. Change the observing port.

   # Change the observing port to XGigabitEthernet 0/0/5.

   ```
   [Switch] observe-port 1 interface XGigabitEthernet 0/0/5
   ```

5. Configure a mirrored port.

   # Configure XGigabitEthernet 0/0/1 as the mirrored port again.

   ```
   [Switch] interface XGigabitEthernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
   [Switch-XGigabitEthernet0/0/1] quit
   ```

6. Verify the configuration.

   # Run the **display port-mirroring** command. You can check the configurations on the current observing port and mirrored port.

   ```
   [Switch] display port-mirroring
     Port-
   mirror:
   ------------------------------------------------------------
     Mirror-port              Direction     Observe-port
   ------------------------------------------------------------
     XGigabitEthernet0/0/1     Inbound
   XGigabitEthernet0/0/5
   ```

Configuration Files

Configuration file of the Switch

```
#
 sysname Switch
#
 observe-port 1 interface XGigabitEthernet0/0/5
#
interface XGigabitEthernet0/0/1
 port-mirroring to observe-port 1 inbound
#
return
```

8.5 ALS Configuration

This chapter describes the Automatic Laser Shutdown (ALS) configuration on the S6700.

8.5.1 Example for Configuring ALS

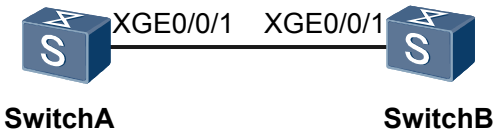
Through the ALS function, a laser can automatically stop sending pulses when a link is faulty and recover pulse transmission after the link is recovered.

Networking Requirements

As shown in **Figure 8-11**, the LPUs that support ALS are installed in slot 1 of Switch A and Switch B, XGE 0/0/1 of Switch A and Switch B are connected through a fiber.

When data transmission is interrupted by faults occurred on the fiber link, if the laser of the optical module sends pulses continuously, the energy is wasted and potential risks are caused. After ALS is enabled on both interfaces of the fiber link, the laser stops sending pulses if a fault occurs on the fiber link. If the faulty link is recovered, the laser starts to send pulses.

Figure 8-11 ALS application



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable ALS on XGE 0/0/1 on Switch A and Switch B.
2. Configure the lasers of XGE 0/0/1 on Switch A and Switch B to work in automatic restart mode.
3. Set the ALS pulse intervals and widths of the lasers of XGE 0/0/1 on Switch A and Switch B.

Data Preparation

To complete the configuration, you need the following data:

- ALS pulse interval and width of the laser of the optical module on XGE 0/0/1 of Switch A
- ALS pulse interval and width of the laser of the optical module on XGE 0/0/1 of Switch B

Procedure

Step 1 Enable ALS on XGE 0/0/1 of Switch A, configure the laser of the interface to work in automatic restart mode, and set the ALS pulse interval and width to 200s and 3s.

Enable ALS.

```
<SwitchA> system-view
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] als enable
```

Set the ALS pulse interval and width of the laser.

```
[SwitchA-XGigabitEthernet0/0/1] undo als restart mode manual
[SwitchA-XGigabitEthernet0/0/1] als restart pulse-interval 200
[SwitchA-XGigabitEthernet0/0/1] als restart pulse-width 3
```

Step 2 Enable ALS on XGE 0/0/1 of Switch B, configure the laser of the interface to work in automatic restart mode, and set the ALS pulse interval and width to 200s and 3s.

Enable ALS.

```
<SwitchB> system-view
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] als enable
```

Set the ALS pulse interval and width of the laser.

```
[SwitchB-XGigabitEthernet0/0/1] undo als restart mode manual
[SwitchB-XGigabitEthernet0/0/1] als restart pulse-interval 200
[SwitchB-XGigabitEthernet0/0/1] als restart pulse-width 3
```

Step 3 Verify the configuration.

Run the **display als configuration interface** *interface-type interface-number* command on Switch A and Switch B to view the ALS configuration.

```
<SwitchA> display als configuration interface xgigabitethernet0/0/1

--------------------------------------------------------------------------------
Interface               ALS        Laser      Restart    Interval(s)   Width(s)
                        Status     Status     Mode
--------------------------------------------------------------------------------
XGigabitEthernet0/0/1    Enable     Off        Auto       200           3
--------------------------------------------------------------------------------
<SwitchB> display als configuration interface xgigabitethernet0/0/1

--------------------------------------------------------------------------------
Interface               ALS        Laser      Restart    Interval(s)   Width(s)
                        Status     Status     Mode
--------------------------------------------------------------------------------
XGigabitEthernet0/0/1    Enable     Off        Auto       200           3
--------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
interface XGigabitEthernet0/0/1
 als enable
 als restart pulse-interval 200
 als restart pulse-width 3
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
interface XGigabitEthernet0/0/1
 als enable
 als restart pulse-interval 200
 als restart pulse-width 3
#
return
```

8.5.2 Establishing the Configuration Task

Before rebooting the S6700, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This helps you complete the configuration task quickly and accurately.

Applicable Environment

After upgrading the S6700, you need to reboot it.

Pre-configuration Tasks

None.

Data Preparation

None.

8.5.3 (Optional) Rebooting the S6700 Through Command Lines

You can use commands to reboot the S6700 immediately.

Context

CAUTION

Be cautious to use the **reboot** command because it can break down the whole network for a short period of time. Before you reboot the S6700 through the **reboot** command, the system compares the current configuration with that saved in the configuration file. If they are not consistent, the system prompts you to save the current configuration. Ensure that correct files are used for rebooting the S6700.

Do as follows on the S6700 that needs to be rebooted immediately:

Procedure

Step 1 Run:

```
reboot [ fast | save diagnostic-information ]
```

The S6700 is rebooted immediately.

By default, this command can only be run by users at the management level.

----End

8.5.4 (Optional) Rebooting the S6700 Immediately by Pressing the Power Button

You can use press the power button to restart the S6700 immediately.

Context

CAUTION

Be cautious to perform this operation because it can break down the entire network for a short period of time. Before you reboot the S6700 through the power button, check whether configuration files need be saved and ensure that correct files are used for rebooting the S6700. For details on saving configuration files, see the *Quidway S6700 Series Ethernet Switches Configuration Guide - Basic Configuration*.

Do as follows on the S6700 that needs to be rebooted immediately:

Procedure

Step 1 Press the **RST** button of the S6700 to reboot theS6700.

----End

8.5.5 (Optional) Rebooting the S6700 on Schedule Using Command Lines

You can use commands to reboot the S6700 on schedule.

Context

CAUTION

Be cautious to use the **schedule reboot** command because it can break down the whole network for a short period of time.

Before you run the **schedule reboot** command to reboot the S6700 on schedule, check whether configuration files need be saved and ensure that correct files are used for rebooting the S6700. For details on saving configuration files, see the *Quidway S6700 Series Ethernet Switches Configuration Guide - Basic Configuration*.

Do as follows on the S6700 that needs to be rebooted on schedule:

Procedure

Step 1 Run:

On-schedule reboot is configured. You can specify the time for rebooting theS6700 by setting *type*.

- **at** *time*: specifies the specific time for rebooting the S6700.
- **delay** *interval*: specifies the waiting time before rebooting the S6700.

By default, this command can only be run by users at the management level. By default, the time for rebooting the S6700 is not set. That is, on-schedule reboot is not enabled.

----End

8.5.6 Checking the Configuration

After using commands to reboot the S6700 on schedule, you can view information about on-schedule reboot of the S6700.

Prerequisite

On-schedule reboot has been enabled through command lines.

Procedure

Step 1 Run the **display schedule reboot** command to check configurations about on-schedule reboot of the S6700.

----End

Example

If information about on-schedule reboot of the S6700 is displayed, it means that the configuration succeeds.

```
<Quidway> display schedule reboot
Info:System will reboot at 00:00:00 2007/10/30 (in 23 hours and 53 minutes).
```

9 Configuration Guide - Network Management

About This Chapter

This document describes the configuration procedures and configuration examples of the SNMP, RMON,NTP, LLDP, NQA and Ping and Tracert features on the S6700. The document provides guides to configure the network management functions of the S6700.

9.1 SNMP Configuration
The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. There are three SNMP versions, SNMPv1, SNMPv2c, and SNMPv3. Users can choose to configure one or more versions if needed.

9.2 LLDP Configuration
This chapter describes the LLDP concept, configuration procedures, and configuration examples.

9.3 HGMP Configuration
By running the Huawei Group Management Protocol (HGMP), you can appoint a switch as the administrator switch to create a cluster and add a large number of Ethernet switches to the cluster. The administrator is used to perform unified management and configuration over these switches, which simplifies maintenance and engineering.

9.4 NTP Configuration
This chapter describes how to configure Network Time Protocol (NTP) to make clocks of the devices on the network identical.

9.5 Ping and Tracert
This chapter describes basic concepts and applications of the **ping** and **tracert** commands.

9.6 NQA Configuration
This chapter describes how to configure the Network Quality Analysis (NQA) to monitor the network operating status and collect network operation indexes in real time.

9.7 RMON Configuration

This chapter describes how to monitor the Ethernet interface through Remote Network Monitoring (RMON).

9.1 SNMP Configuration

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. There are three SNMP versions, SNMPv1, SNMPv2c, and SNMPv3. Users can choose to configure one or more versions if needed.

9.1.1 Example for Configuring a Device to Communicate with an NM Station by Using SNMPv1

This section provides an example to describe how to configure a device to communicate with an NM station by using SNMPv1 and how to specify the MIB objects that can be managed by the NM station.

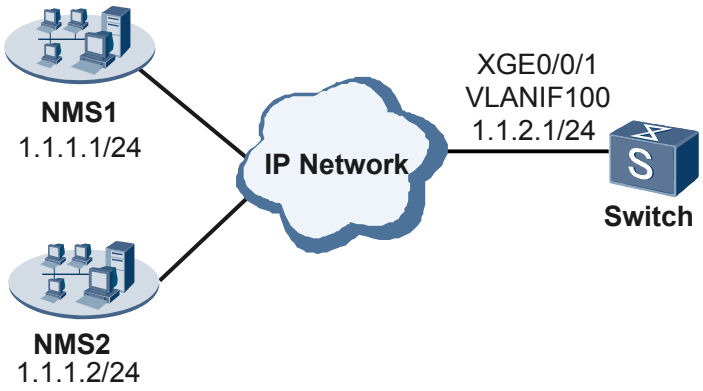
Networking Requirements

As shown in **Figure 9-1**, two NM stations (NMS1 and NMS2) and the switch are connected across a public network. According to the network planning, NMS2 can manage every MIB object except HGMP on the switch, and NMS1 does not manage the switch.

On the switch, only the modules that are enabled by default are allowed to send alarms to NMS2. This prevents an excess of unwanted alarms from being sent to NMS2. Excessive alarms can make faults location difficult.

Equipment administrator's contact information needs to be configured on the switch. This allows the NMS administrator to contact the equipment administrator quickly if a fault occurs.

Figure 9-1 Networking diagram for configuring a device to communicate with an NM station by using SNMPv1



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the SNMP agent.

2. Configure the switch to run SNMPv1.
3. Configure an ACL to allow NMS2 to manage every MIB object except HGMP on the switch.
4. Configure the trap function to allow the switch to send alarms to NMS2.
5. Configure the equipment administrator's contact information on the switch.
6. Configure NMS2.

Data Preparation

To complete the configuration, you need the following data:

- SNMP version
- Community name
- ACL number
- IP address of the NM station
- Equipment administrator's contact information

Procedure

Step 1 Configure available routes between the switch and the NM stations. Details for the configuration procedure are not provided here.

Step 2 Enable the SNMP agent.

```
<Quidway> system-view
[Quidway] snmp-agent
```

Step 3 Configure the switch to run SNMPv1.

```
[Quidway] snmp-agent sys-info version v1
```

Check the configured SNMP version.

```
[Quidway] display snmp-agent sys-info version
SNMP version running in the system:
            SNMPv1 SNMPv3
```

Step 4 Configure the NM stations' access rights.

Configure an ACL to allow NMS2 to manage and disallow NMS1 from managing the switch.

```
[Quidway] acl 2001
[Quidway-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Quidway-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

Configure a MIB view and allow NMS2 to manage every MIB object except HGMP on the switch.

```
[Quidway] snmp-agent mib-view excluded allexthgmp 1.3.6.1.4.1.2011.6.7
```

Configure a community name to allow NMS2 to manage the objects in the MIB view.

```
[Quidway] snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
```

Step 5 Configure the trap function.

```
[Quidway] snmp-agent target-host trap address udp-domain 1.1.1.2 params
securityname 1.1.3.1
[Quidway] snmp-agent trap source Loopback0
```

```
[Quidway] snmp-agent trap queue-size 200
[Quidway] snmp-agent trap life 60
```

Step 6 Configure the equipment administrator's contact information.

```
[Quidway] snmp-agent sys-info contact call Operator at 010-12345678
```

Step 7 Configure NMS2.

For details on how to configure NMS2, see the relevant NMS configuration guide.

Step 8 Verify the configuration.

After the configurations are complete, run the following commands to verify that the configurations have taken effect.

Check information about the SNMP community name.

```
<Quidway> display snmp-agent community
   Community name:adminnms2
       Group name:adminnms2
       Acl:2001
       Storage-type: nonVolatile
```

Check the configured ACL.

```
<Quidway> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

Check the MIB view.

```
<Quidway> display snmp-agent mib-view viewname allexthgmp
View name:allexthgmp
       MIB Subtree:hwCluster
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
```

Check the target host.

```
<Quidway> display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
  IP-address       : 1.1.1.2
  Source interface : -
  VPN instance     : -
  Security name    : 1.1.3.1
  Port             : 162
  Type             : trap
  Version          : v1
  Level            : No authentication and privacy
  NMS type         : NMS
------------------------------------------------------------
```

When an alarm is generated, run the **display trapbuffer** command to view the details.

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
```

```
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

Check the equipment administrator's contact information.

```
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----End

Configuration Files

Configuration file of the switch

```
#
 vlan batch 100
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface Vlanif100
 ip address 1.1.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface LoopBack0
 ip address 1.1.3.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
  network 1.1.3.1 0.0.0.0
 #
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v1  v3
 snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname
1.1.3.1

 snmp-agent mib-view excluded allexthgmp hwCluster
 snmp-agent trap source LoopBack0
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
#
return
```

9.1.2 Example for Configuring a Device to Communicate with an NM Station by Using SNMPv2c

This section provides an example to describe how to configure a device to communicate with an NM station by using SNMPv2c and how to specify the MIB objects that can be managed by the NM station.

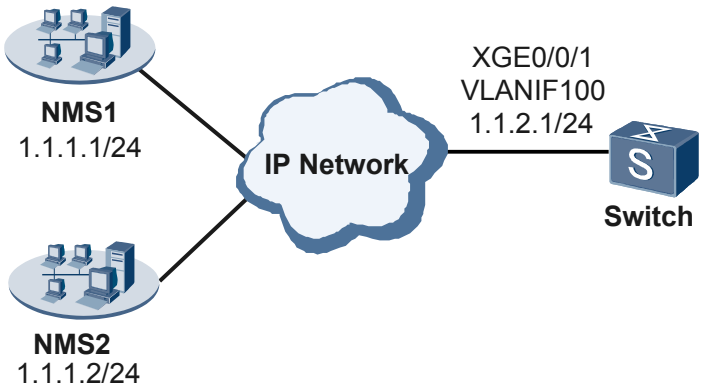
Networking Requirements

As shown in **Figure 9-2**, two NM stations (NMS1 and NMS2) and the switch are connected across a public network. According to the network planning, NMS2 can manage every MIB object except HGMP on the switch, and NMS1 does not manage the switch.

On the switch, only the modules that are enabled by default are allowed to send alarms to NMS2. This prevents an excess of unwanted alarms from being sent to NMS2. Excessive alarms can make faults location difficult. Informs need to be used to ensure that alarms are received by NMS2 because alarms sent by the switch have to travel across the public network to reach NMS2.

Equipment administrator's contact information needs to be configured on the switch. This allows the NMS administrator to contact the equipment administrator quickly if a fault occurs.

Figure 9-2 Networking diagram for configuring a device to communicate with an NM station by using SNMPv2c



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the SNMP agent.
2. Configure the switch to run SNMPv2c.
3. Configure an ACL to allow NMS2 to manage every MIB object except HGMP on the switch.
4. Configure the switch to send informs to NMS2 to ensure alarm sending reliability.
5. Configure the equipment administrator's contact information on the switch.
6. Configure NMS2.

Data Preparation

To complete the configuration, you need the following data:

- SNMP version
- Community name
- ACL number
- IP address of the NM station
- Equipment administrator's contact information

Procedure

Step 1 Configure available routes between the switch and the NM stations. Details for the configuration procedure are not provided here.

Step 2 Enable the SNMP agent.

```
<Quidway> system-view
[Quidway] snmp-agent
```

Step 3 Configure the switch to run SNMPv2c.

```
[Quidway] snmp-agent sys-info version v2c
```

Check the configured SNMP version.

```
[Quidway] display snmp-agent sys-info version
SNMP version running in the system:
           SNMPv2c SNMPv3
```

Step 4 Configure the NM stations' access rights.

Configure an ACL to allow NMS2 to manage and disallow NMS1 from managing the switch.

```
[Quidway] acl 2001
[Quidway-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Quidway-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

Configure a MIB view.

```
[Quidway] snmp-agent mib-view excluded allexthgmp 1.3.6.1.4.1.2011.6.7
```

Configure a community name to allow NMS2 to manage the objects in the MIB view.

```
[Quidway] snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
```

Step 5 Configure the trap function.

```
[Quidway] snmp-agent target-host inform address udp-domain 1.1.1.2 params
securityname 1.1.2.1 v2c
[Quidway] snmp-agent inform timeout 15 resend-times 3 pending 39
[Quidway] snmp-agent notification-log enable
[Quidway] snmp-agent notification-log global-ageout 12
```

Step 6 Configure the equipment administrator's contact information.

```
[Quidway] snmp-agent sys-info contact call Operator at 010-12345678
```

Step 7 Configure NMS2.

For details on how to configure NMS2, see the relevant NMS configuration guide.

Step 8 Verify the configuration.

After the configurations are complete, run the following commands to verify that the configurations have taken effect.

Check information about the SNMP community name.

```
<Quidway> display snmp-agent community
   Community name:adminnms2
       Group name:adminnms2
       Acl:2001
       Storage-type: nonVolatile
```

Check the configured ACL.

```
<Quidway> display acl 2001
```

```
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

Check the MIB view.

```
<Quidway> display snmp-agent mib-view viewname allexthgmp
View name:allexthgmp
       MIB Subtree:hwCluster
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
```

Check the target host.

```
<Quidway> display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
  IP-address       : 1.1.1.2
  Source interface : -
  VPN instance     : -
  Security name    : 1.1.2.1
  Port             : 162
  Type             : inform
  Version          : v2c
  Level            : No authentication and privacy
  NMS type         : NMS
------------------------------------------------------------
```

When an alarm is generated, run the **display trapbuffer** command to view the details.

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

Check the equipment administrator's contact information.

```
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
           call Operator at 010-12345678
```

----End

Configuration Files

Configuration file of the switch

```
#
 vlan batch 100
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface Vlanif100
 ip address 1.1.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
```

```
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
#
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community write adminnms2 mib-view allexthgmp acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v2c v3
 snmp-agent target-host inform address udp-domain 1.1.1.2 params securityname
1.1.2.1 v2c
 snmp-agent mib-view excluded allexthgmp hwCluster
 snmp-agent inform timeout 15 resend-times 3 pending 39
 snmp-agent notification-log enable
 snmp-agent notification-log global-ageout 12
#
return
```

9.1.3 Example for Configuring a Device to Communicate with an NM Station by Using SNMPv3

This section provides an example to describe how to configure a device to communicate with an NM station by using SNMPv3 and how to specify the MIB objects that can be managed by the NM station.

Networking Requirements

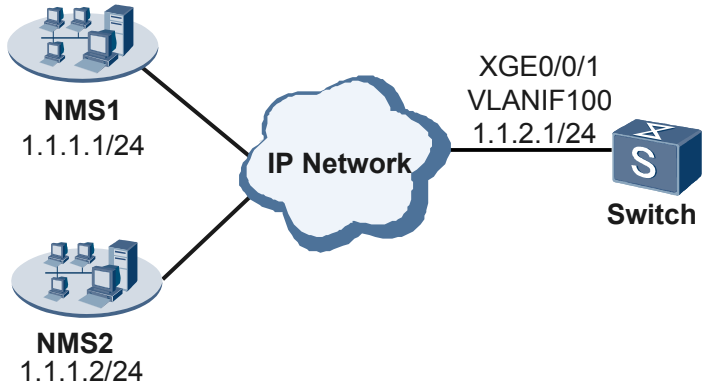
As shown in **Figure 9-3**, two NM stations (NMS1 and NMS2) and the switch are connected across a public network. According to the network planning, NMS2 can manage every MIB object except HGMP on the switch, and NMS1 does not manage the switch.

On the switch, only the modules that are enabled by default are allowed to send alarms to NMS2. This prevents an excess of unwanted alarms from being sent to NMS2. Excessive alarms can make faults location difficult.

The data transmitted between NMS2 and the switch needs to be encrypted and the NMS administrator needs to be authenticated because the data has to travel across the public network.

Equipment administrator's contact information needs to be configured on the switch. This allows the NMS administrator to contact the equipment administrator quickly if a fault occurs.

Figure 9-3 Networking diagram for configuring a device to communicate with an NM station by using SNMPv3



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the SNMP agent.
2. Configure the switch to run SNMPv3.
3. Configure an ACL to allow NMS2 to manage every MIB object except HGMP on the switch and configure data encryption.
4. Configure the trap function to allow the switch to send alarms to NMS2.
5. Configure the equipment administrator's contact information on the switch.
6. Configure NMS2.

Data Preparation

To complete the configuration, you need the following data:

- SNMP version
- User group name
- User name and password
- Authentication and encryption algorithms
- ACL number
- IP address of the NM station
- Equipment administrator's contact information

Procedure

Step 1 Configure available routes between the switch and the NM stations. Details for the configuration procedure are not provided here.

Step 2 Enable the SNMP agent.

```
<Quidway> system-view
[Quidway] snmp-agent
```

Step 3 Configure the switch to run SNMPv3.

```
[Quidway] snmp-agent sys-info version v3
```

Check the configured SNMP version.

```
[Quidway] display snmp-agent sys-info version
SNMP version running in the system:
           SNMPv3
```

Step 4 Configure the NM stations' access rights.

Configure an ACL to allow NMS2 to manage and disallow NMS1 from managing the switch.

```
[Quidway] acl 2001
[Quidway-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Quidway-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Quidway-acl-basic-2001] quit
```

Configure a MIB view.

```
[Quidway] snmp-agent mib-view included testview iso
```

Configure an SNMPv3 user group and add a user to the group, and configure authentication for the NMS administrator and encryption for the data transmitted between the switch and NMS2.

```
[Quidway] snmp-agent usm-user v3 testuser testgroup authentication-mode md5
87654321 privacy-mode des56 87654321
[Quidway] snmp-agent group v3 testgroup privacy write-view testview notify-view
testview acl 2001
```

Step 5 Configure the trap function.

```
[Quidway] snmp-agent target-host trap address udp-domain 1.1.1.2 params
securityname testuser
[Quidway] snmp-agent trap source loopback0
[Quidway] snmp-agent trap queue-size 200
[Quidway] snmp-agent trap life 60
```

Step 6 Configure the equipment administrator's contact information.

```
[Quidway] snmp-agent sys-info contact call Operator at 010-12345678
```

Step 7 Configure the NMS2.

For details on how to configure NMS2, see the relevant NMS configuration guide.

Step 8 Verify the configuration.

After the configurations are complete, run the following commands to verify that the configurations have taken effect.

Check information about the user group.

```
<Quidway> display snmp-agent group testgroup

   Group name: testgroup
       Security model: v3 AuthPriv
       Readview: ViewDefault
       Writeview: testview
       Notifyview: testview
       Storage-type: nonVolatile
       Acl:2001
```

Check information about the user.

```
<Quidway> display snmp-agent usm-user

       User name: testuser
       Engine ID: 000007DB7F00000100004C3F active
       Group name:testgroup
```

Check the configured ACL.

```
<Quidway> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

Check the MIB view.

```
<Quidway> display snmp-agent mib-view viewname testview
       View name:testview
       MIB Subtree:iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active
```

Check the target host.

```
<Quidway> display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
  IP-address       : 1.1.1.2
  Source interface : -
  VPN instance     : -
  Security name    : testuser
  Port             : 162
  Type             : trap
  Version          : v1
  Level            : No authentication and privacy
  NMS type         : NMS
------------------------------------------------------------
```

When an alarm is generated, run the **display trapbuffer** command to view the details.

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59 RouterA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

Check the equipment administrator's contact information.

```
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
           call Operator at 010-12345678
```

----End

Configuration Files

Configuration file of the switch

```
#
 vlan batch 100
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface Vlanif100
 ip address 1.1.2.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface LoopBack0
 ip address 1.1.3.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
  network 1.1.3.1 0.0.0.0
#
 snmp-agent
 snmp-agent local-engineid 000007DB7FFFFFFF000004A7
 snmp-agent sys-info contact call Operator at 010-12345678
```

```
 snmp-agent sys-info version v3
 snmp-agent group v3 testgroup privacy  write-view testview notify-view testview
acl 2001
 snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname
testuser
 snmp-agent mib-view included testview iso
 snmp-agent usm-user v3 testuser testgroup authentication-mode md5 N'!2Z
[^HZ0T&P'@XIM=F#Q!! privacy-mode des56 N'!2Z[^HZ0T&P'@XIM=F#Q!!
 snmp-agent trap source LoopBack0
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
#
return
```

9.2 LLDP Configuration

This chapter describes the LLDP concept, configuration procedures, and configuration examples.

9.2.1 Example for Configuring LLDP on the Device That Has a Single Neighbor

After LLDP is configured on the network devices, the NMS can obtain the network topology. The following example describes how to configure LLDP on the devices that have a single neighbor.

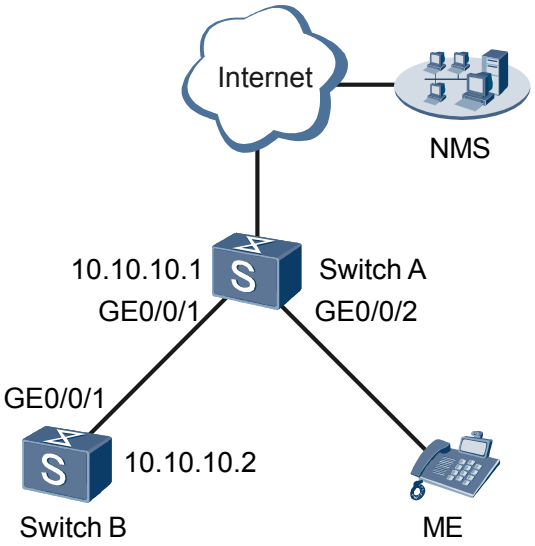
Networking Requirements

As shown in **Figure 9-4**, SwitchA is directly connected to SwitchB and media endpoint (ME). The NMS needs to obtain Layer 2 information about SwitchA, SwitchB, and ME. By using the Layer 2 information, a network administrator can know the detailed network topology information and configuration conflicts. These requirements can be met by configuring LLDP on SwitchA and SwitchB.

In addition, the administrator requires that SwitchA and SwitchB send LLDP traps to the NMS when the LLDP management address changes, global LLDP is enabled or disabled, or the neighbor information changes. This ensures that the administrator detects topology changes in time.

The ME supports the LLDP function. Reachable routes exist between the NMS and Switches. The SNMP parameters are set on all devices.

Figure 9-4 Configuring LLDP on the device that has a single neighbor



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable global LLDP on SwitchA and SwitchB.
2. Enable SwitchA and SwitchB to process LLDP BPDUs.
3. Configure management addresses for SwitchA and SwitchB.
4. Enable the LLDP trap function on SwitchA and SwitchB.

Data Preparation

To complete the configuration, you need the following data:

- Management address 10.10.10.1 for SwitchA and management address 10.10.10.2 for SwitchB

Procedure

Step 1 Enable global LLDP on SwitchA and SwitchB.

Configure SwitchA.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] lldp enable
```

Configure SwitchB.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] lldp enable
```

Step 2 Enable SwitchA and SwitchB to process LLDP BPDUs.

Configure SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] bpdu enable
```

Configure SwitchB.

```
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] bpdu enable
```

Step 3 Configure management addresses for SwitchA and SwitchB.

Configure SwitchA.

```
[SwitchA] lldp management-address 10.10.10.1
```

Configure SwitchB.

```
[SwitchB] lldp management-address 10.10.10.2
```

Step 4 Enable the LLDP trap function on SwitchA and SwitchB.

Configure SwitchA.

```
[SwitchA] snmp-agent trap enable feature-name lldptrap
```

Configure SwitchB.

```
[SwitchB] snmp-agent trap enable feature-name lldptrap
```

Step 5 Verify the configuration.

Check whether the LLDP function is enabled, management addresses are configured, and the LLDP trap function is enabled.

- View the configurations on SwitchA.

```
[SwitchA] display lldp local
System
information
Chassis
type   :macAddress
Chassis ID     :00e0-
fc33-0011
System name    :SwitchA
System description  :Quidway
Huawei Versatile Routing Platform
Software
VRP (R) Software, Version 5.70 (S6700 V200R006C00)
Copyright (c) 2003-2010 Huawei Technologies Co.,
Ltd

System capabilities
supported   :bridge
System capabilities
enabled     :bridge
LLDP Up time   :2009/2/13
18:31:37

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :VER B
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V200R006C00

SerialNum         :NA
Manufacturer name :NA
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                    :enabled            (default is disabled)
```

```
LLDP Message Tx Interval        :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                  (default is 4)
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is disabled)
Management Address              :IP: 10.10.10.1

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 0 hours, 0 minutes, 0 seconds

Remote Neighbors Added          :0

Remote Neighbors Deleted        :0

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :1
Port information:


Port information:

Interface XGigabitEthernet0/0/1:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :XGigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/1 Interface


Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

View the neighbor information of SwitchA.

```
<SwitchA> display lldp neighbor interface xgigabitethernet 0/0/1
XGigabitEthernet0/0/1 has 1 neighbors:


Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0011
Port ID type   :interfaceName
Port ID        :XGigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/1 Interface
System name         :SwitchB
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (S6700 V200R006C00)
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.2
Expired time   :118s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :LE01MCUA VER.A
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V200R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID      :0
Media policy L2 priority :0
Media policy Dscp        :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

- View the configurations on SwitchB.

Similar to information about SwitchA.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 lldp enable
#
interface XGigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
 lldp management-address  10.10.10.1
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
 lldp enable
#
interface XGigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
 lldp management-address 10.10.10.2
#
return
```

9.2.2 Example for Configuring LLDP on the Device That Has Multiple Neighbors

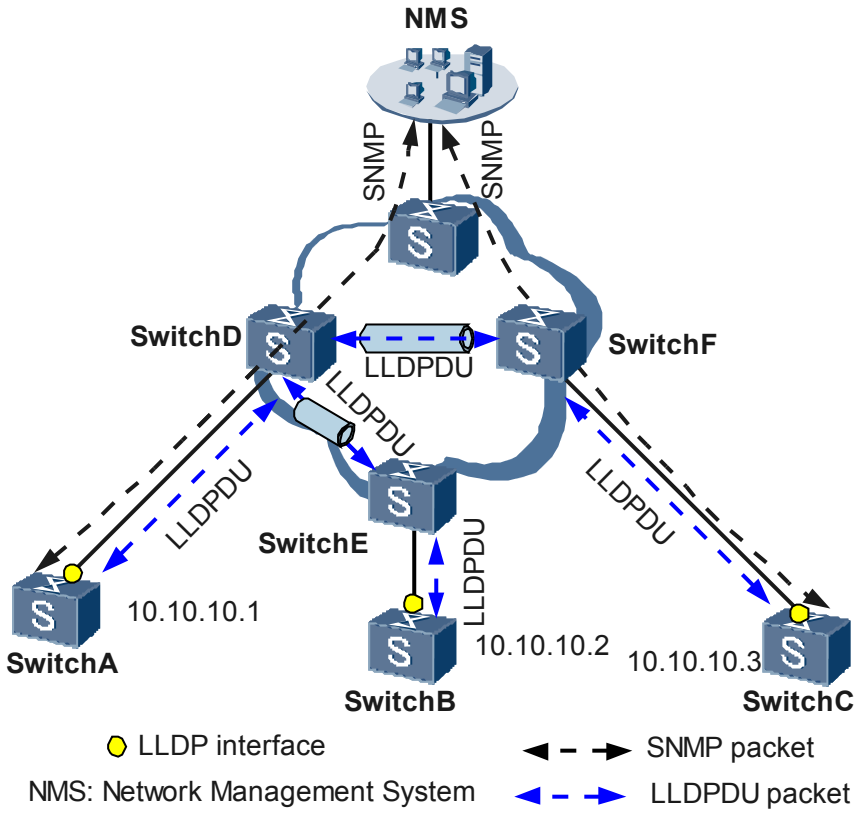
After LLDP is configured on the network devices, the NMS can obtain the network topology. The following example describes how to configure LLDP on the devices that have multiple neighbors.

Networking Requirements

As shown in **Figure 9-5**, SwitchA, SwitchB, and SwitchC are connected through an unknown network. The unknown network is not managed by the NMS, but can transparently transmit LLDP packets. The NMS needs to obtain Layer 2 information about SwitchA, SwitchB, and SwitchC. By using the Layer 2 information, a network administrator can know the detailed network topology information and configuration conflicts. These requirements can be met by configuring LLDP on SwitchA, SwitchB, and SwitchC.

The NMS has reachable routes to SwitchA, SwitchB, and SwitchC and SNMP parameters are set on all devices.

Figure 9-5 Configuring LLDP on the device that has multiple neighbors



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable global LLDP on SwitchA, SwitchB, and SwitchC.
2. Enable SwitchA, SwitchB, and SwitchC to process LLDP BPDUs.
3. Configure management addresses for SwitchA, SwitchB, and SwitchC.

Data Preparation

To complete the configuration, you need the following data:

- Management addresses for SwitchA, SwitchB, and SwitchC

Procedure

Step 1 Enable global LLDP on SwitchA, SwitchB, and SwitchC.

Configure SwitchA.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] lldp enable
```

Configure SwitchB.

Same as the configurations on SwitchA.

Configure SwitchC.

Same as the configurations on SwitchA.

Step 2 Enable SwitchA, SwitchB, and SwitchC to process LLDP BPDUs.

Configure SwitchA.

```
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-interface XGigabitEthernet0/0/1] bpdu enable
```

Configure SwitchB.

Same as the configurations on SwitchA.

Configure SwitchC.

Same as the configurations on SwitchA.

Step 3 Configure management addresses for SwitchA, SwitchB, and SwitchC.

Configure SwitchA.

```
[SwitchA] lldp management-address 10.10.10.1
```

Configure SwitchB.

```
[SwitchB] lldp management-address 10.10.10.2
```

Configure SwitchC.

```
[SwitchC] lldp management-address 10.10.10.3
```

Step 4 Verify the configuration.

Check whether LLDP function is enabled and management addresses are configured.

- View the configurations on SwitchA.

  # View the neighbor information of SwitchA.

```
<SwitchA> display lldp neighbor interface xgigabitethernet 0/0/1
XGigabitEthernet0/0/1 has 2 neighbors:


Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0012
Port ID type   :interfaceName
Port ID        :XGigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/1 Interface
System name         :SwitchB
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (S6700 )
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.2
Expired time   :118s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM
```

```
Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :VER B
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V200R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Unknown
Unknown Policy      :Undefined
VLAN tagged         :No
Media policy VlanID      :0
Media policy L2 priority :0
Media policy Dscp        :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Neighbor index : 2
Chassis type   :macAddress
Chassis ID     :00e0-fc33-0013
Port ID type   :interfaceName
Port ID        :XGigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/1 Interface
System name         :SwitchC
System description  :Quidway
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.70 (S6700 )
Copyright (c) 2003-2010 Huawei Technologies Co., Ltd

System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.3
Expired time   :118s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
```

```
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :VER B
FirmwareRev       :NC
SoftwareRev       :Version 5.70 V200R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Unknown
Unknown Policy      :Undefined
VLAN tagged         :No
Media policy VlanID      :0
Media policy L2 priority :0
Media policy Dscp        :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

- View the configurations on SwitchB.

  Same as information about SwitchA.

- View the configurations on SwitchC.

  Same as information about SwitchA.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
#
 lldp enable
#
 lldp management-address 10.10.10.1
#
interface XGigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
#
 lldp enable
#
 lldp management-address 10.10.10.2
#
```

```
interface XGigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
return
```

- Configuration file of SwitchC

```
#
 sysname SwitchC
#
#
 lldp enable
#
 lldp management-address 10.10.10.3
#
interface XGigabitEthernet0/0/1
 undo port hybrid vlan 1
 bpdu enable
#
return
```

9.2.3 Example for Configuring LLDP on the Network Where Link Aggregation Is Configured

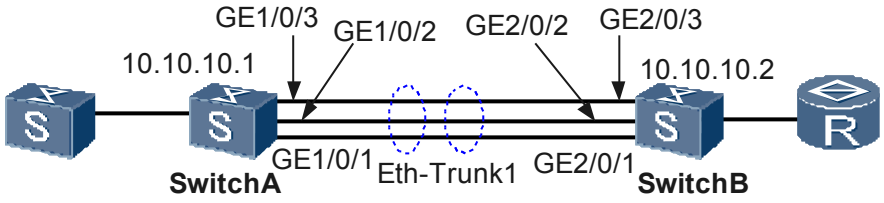
After LLDP is configured on the interfaces of network devices, the NMS can obtain the network topology. The following example describes how to configure LLDP on the network where link aggregation is configured.

Networking Requirements

As shown in **Figure 9-6**, SwitchA and SwitchB need to be connected by an Eth-Trunk. The NMS needs to obtain the Layer 2 information between the Switches. By using the Layer 2 information, a network administrator can know the detailed topology information and configuration errors on the devices outside the unknown network. These requirements can be met by configuring LLDP on SwitchA and SwitchB.

The NMS has reachable routes to SwitchA and SwitchB and SNMP parameters are set on all devices.

Figure 9-6 Configuring LLDP on the network where link aggregation is configured



Configuration Roadmap

The configuration roadmap is as follows:

1. Add the physical interfaces of SwitchA and SwitchB to the Eth-Trunk.
2. Enable global LLDP on SwitchA and SwitchB.

3. Enable SwitchA and SwitchB to process LLDP BPDUs.
4. Configure management addresses for SwitchA and SwitchB.

Data Preparation

To complete the configuration, you need the following data:

- Management address 10.10.10.1 for SwitchA and management address 10.10.10.2 for SwitchB
- Number of the Eth-Trunk between SwitchA and SwitchB, and numbers of the interfaces added to the Eth-Trunk

Procedure

Step 1 Configure the Eth-Trunk between SwitchA and SwitchB.

Configure SwitchA.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] trunkport xgigabitethernet 0/0/1
[SwitchA-Eth-Trunk1] trunkport xgigabitethernet 0/0/2
[SwitchA-Eth-Trunk1] trunkport xgigabitethernet 0/0/3
[SwitchA-Eth-Trunk1] port link-type trunk
[SwitchA-Eth-Trunk1] port trunk allow-pass vlan 100
[SwitchA-Eth-Trunk1] quit
```

Configure SwitchB.

Same as the configurations on SwitchA.

Step 2 Enable global LLDP on SwitchA and SwitchB.

Configure SwitchA.

```
[SwitchA] lldp enable
```

Configure SwitchB.

Same as the configurations on SwitchA.

Step 3 Enable SwitchA and SwitchB to process LLDP BPDUs.

Configure SwitchA.

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] bpdu enable
[SwitchA-Eth-Trunk1] quit
```

Configure SwitchB.

Same as the configurations on SwitchA.

Step 4 Configure management addresses for SwitchA and SwitchB.

Configure SwitchA.

```
[SwitchA] lldp management-address 10.10.10.1
```

Configure SwitchB.

```
[SwitchB] lldp management-address 10.10.10.2
```

Step 5 Verify the configuration.

- View the configurations on SwitchA.

  # Check whether the physical interfaces are added to Eth-Trunk1.

```
[SwitchA] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-
DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber:
8
Operate status: up          Number Of Up Port In Trunk:
3
--------------------------------------------------------------------------------
-
PortName                      Status
Weight
XGigabitEthernet0/0/1          Up
1
XGigabitEthernet0/0/2          Up          1
XGigabitEthernet0/0/3          Up          1
```

  # View the LLDP configurations.

```
[SwitchA] display lldp local
System
information
Chassis
type   :macAddress
Chassis ID     :00e0-
fc33-0011
System name    :SwitchA
System description  :Quidway
Huawei Versatile Routing Platform
Software
VRP (R) Software, Version 5.70 (S6700 V200R006C00)
Copyright (c) 2003-2010 Huawei Technologies Co.,
Ltd

System capabilities
supported   :bridge
System capabilities
enabled     :bridge
LLDP Up time   :2010/2/13
18:31:37

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :VER B
FirmwareRev       :NA
SoftwareRev       :Version 5.70 V200R006C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                     :enabled             (default is disabled)
LLDP Message Tx Interval        :30                  (default is 30s)
LLDP Message Tx Hold Multiplier :4                   (default is 4)
LLDP Refresh Delay              :2                   (default is 2s)
LLDP Tx Delay                   :2                   (default is 2s)
LLDP Notification Interval      :5                   (default is 5s)
LLDP Notification Enable        :enabled             (default is disabled)
Management Address              :IP: 10.10.10.1

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 15 hours, 1 minutes, 21 seconds
```

```
Remote Neighbors Added          :1

Remote Neighbors Deleted        :0

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:

Interface XGigabitEthernet0/0/1:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :XGigabitEthernet0/0/1
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/1 Interface

Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN Name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :1
Maximum frame Size       :1600

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Interface XGigabitEthernet0/0/2:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors           :1

Port ID subtype     :interfaceName
Port ID             :XGigabitEthernet0/0/2
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/2 Interface

Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN Name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM
```

```
Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :Yes
Aggregation port ID      :1
Maximum frame Size       :1600

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Interface XGigabitEthernet0/0/3:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors           :1

Port ID subtype     :interfaceName
Port ID             :XGigabitEthernet0/0/3
Port description    :HUAWEI, Quidway Series, XGigabitEthernet0/0/3 Interface

Port And Protocol vlan ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN Name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :Yes
Aggregation port ID      :1
Maximum frame Size       :1600

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
```

```
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
```

View the neighbor information of SwitchA.

```
[SwitchA] display lldp neighbor brief
Local Intf   Neighbor Dev             Neighbor Intf
Exptime
XGE0/0/1      SwitchB                  XGE0/0/1                  115
XGE0/0/2      SwitchB                  XGE0/0/2                  115
XGE0/0/3      SwitchB                  XGE0/0/3                  115
```

- View the configurations on SwitchB.

  Same as information about SwitchA.

----End

Configuration Files

- Configuration file of SwitchA

```
#
 sysname SwitchA
#
 vlan batch 100
#
interface MEth0/0/1
 ip address 10.10.10.1 255.255.255.0
#
 lldp enable
#
interface Eth-Trunk1
 port link-type
trunk
 port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/1
 eth-trunk 1
#
interface XGigabitEthernet0/0/2
 eth-trunk 1
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
 lldp management-address  10.10.10.1
#
return
```

- Configuration file of SwitchB

```
#
 sysname SwitchB
#
interface MEth0/0/1
 ip address 10.10.10.2 255.255.255.0
#
 vlan batch 100
#
 lldp enable
#
interface Eth-Trunk1
 port link-type
trunk
 port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/1
 eth-trunk 1
#
interface XGigabitEthernet0/0/2
```

```
 eth-trunk 1
#
interface XGigabitEthernet0/0/3
 eth-trunk 1
#
 lldp management-address  10.10.10.2
#
return
```

9.3 HGMP Configuration

By running the Huawei Group Management Protocol (HGMP), you can appoint a switch as the administrator switch to create a cluster and add a large number of Ethernet switches to the cluster. The administrator is used to perform unified management and configuration over these switches, which simplifies maintenance and engineering.

9.3.1 Example for Configuring Basic HGMP Functions for a Cluster

Networking Requirements

As shown in **Figure 9-7**, a carrier sets up a Layer 2 network through Layer 2 devices. Too many Layer 2 devices are hard to be maintained and managed on the site. In addition, to save public IP addresses, you cannot assign a public IP address to each device.

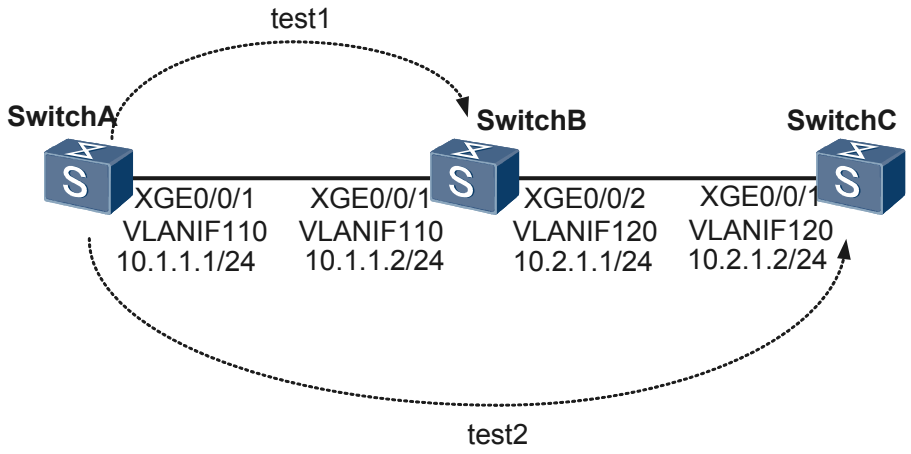
To effectively manage the Layer 2 network, you can create a cluster for the Layer 2 network and manage the cluster through HGMP.

In this example, Administrator-1 is nearest to the network administrator and is therefore appointed as the administrator switch.

NOTE

For convenience, only four devices in the Layer 2 network are described.

Figure 9-7 Networking diagram of configuring basic HGMP functions for a cluster



Device	MAC address	Device	MAC address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002

Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a management VLAN on all devices. Enable NDP and NTDP to ensure that each device can detect the topology structure of the network through NTDP.
2. Choose the administrator switch, and then create a cluster named HUAWEI on the administrator switch.
3. Add all the devices that support HGMP in the Layer 2 network to the cluster.
4. Assign an IP address to VLANIF 10 to facilitate the communication between member switches in the cluster and devices out of the cluster.
5. Configure public servers and hosts for the cluster.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of VLANIF 10, that is 1.0.0.1/8
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator in the cluster, that is 10.0.0.1/8
- MAC addresses of devices, as shown in **Figure 9-7**
- IP addresses of servers and hosts, as shown in **Figure 9-7**

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
```

```
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
```

```
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
```

```
 0003-0003-0003  1                       S6700
 0002-0002-0002  1                       S6700
 0001-0001-0001  0                       S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                 PLATFORM
0004-0004-0004  2                       S6700
0003-0003-0003  1                       S6700
0002-0002-0002  1                       S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   S6700
Member-2                      1     0003-0003-0003   S6700
Member-3                      2     0004-0004-0004   S6700
```

```
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
-------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp server 2.0.0.2
```

```
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
```

```
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

9.3.2 Example for Configuring the Interconnection of FTP Servers and Devices in and out of the HGMP Cluster (in NAT Mode)

Networking Requirements

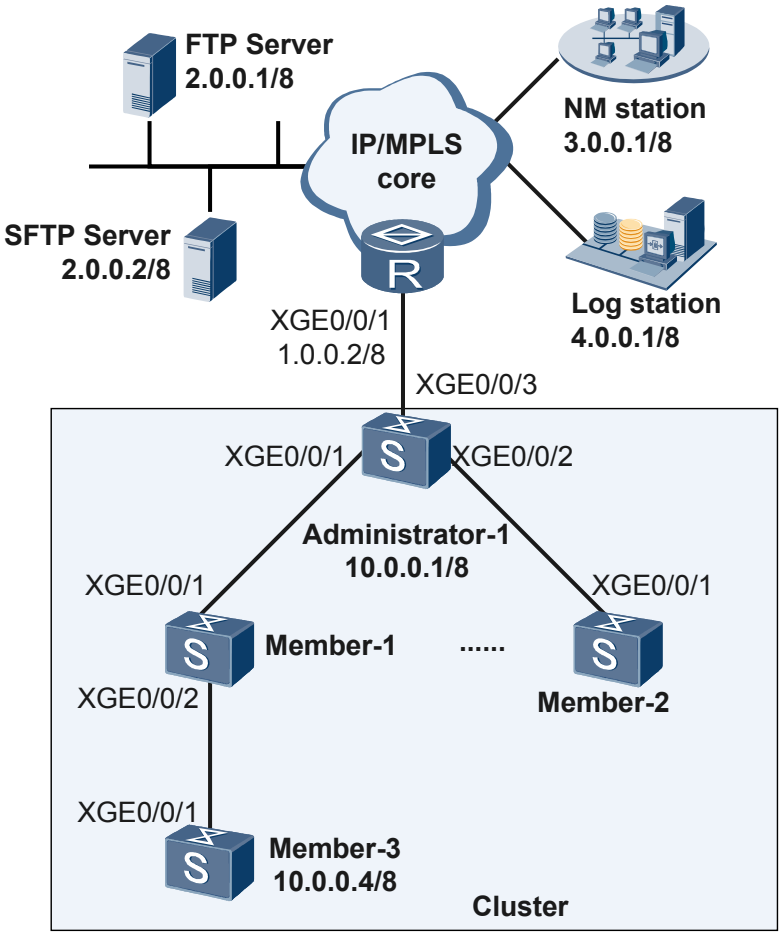
As shown in **Figure 9-8**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-1 is 1, the member ID of Member-2 is 2 and the member ID of Member-3 is 3.

To upload files to Member-1, Member-2, and Member-3 or download files from them, you can set up an FTP connection between the devices out of the cluster and member switches in NAT or non-NAT mode.

NOTE

In this configuration example where the NAT mode is adopted, Member-3 accesses the FTP server (2.0.0.1/8) out of the cluster and devices out of the cluster access the FTP server (Member-2) in the cluster.

Figure 9-8 Networking diagram of configuring the interconnection of FTP servers and devices in and out of the HGMP cluster (in NAT Mode)



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster and configure basic HGMP functions for the cluster according to the steps described in the section "**Example for Configuring Basic HGMP Functions for a Cluster**."
2. For the situation that Member-3 accesses the FTP server (2.0.0.1/8) out of the cluster:
   - Run the **cluster-ftp** command on the member switch to set up a connection with the public FTP server of the cluster.
3. For the situation that a device out of the cluster accesses the FTP server (Member-2):
   - Calculate the port number reserved on the administrator switch for the FTP protocol of a certain member switch in the cluster.

- Run the FTP client program on the PC and create an FTP connection with the member switch.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the FTP server
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8
- Member-2 serving as the FTP server in the cluster with the member ID being 2

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
```

```
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
```

```
      MAC Address : 0002-0002-0002
      Port Name   : XGigabitEthernet0/0/1
      Software Version: Version 5.70 V200R006C00
      Device Name : Member-1
      Port Duplex : FULL
      Product Ver : S6700
Interface: XGigabitEthernet0/0/2
   Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
   Neighbor 1:  Aging Time: 5(s)
      MAC Address : 0003-0003-0003
      Port Name   : XGigabitEthernet0/0/1
      Software Version: Version 5.70 V200R006C00
      Device Name : Member-2
      Port Duplex : FULL
      Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
```

```
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                            Hop   MAC Address     DeviceType
Member-1                        1     0002-0002-0002   S6700
Member-2                        1     0003-0003-0003   S6700
Member-3                        2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
```

```
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Verify the configuration.

- Member switches access the FTP server in NAT mode.

```
<HUAWEI_3.Member-3> cluster-ftp
Trying 10.0.0.1 ...
Press CTRL+K to abort
Connected to 10.0.0.1.
220 FTP service ready.
User(10.0.0.1:(none)):hgmp
331 Password required for hgmp.
Enter password:
230 User logged in.
[ftp]
```

- A device out of the cluster accesses the FTP server in the cluster in NAT mode.

  # Configure an FTP server on Member-2. The configuration details see Configuration Files, and are not mentioned here.

  # Calculate the port number reserved for the FTP protocol of a member switch in the cluster.

  The member ID of Member-2 is 2. Using the formula for computing port numbers reserved for a cluster (Interface number reserved for a cluster = Base interface number + Member number*2) , you can obtain that the reserved port number, which is used by Member-2 to enable the FTP server, is 53248 + 2*2 = 53252.

  # Run the FTP client program on the PC and set up an FTP connection with Member-2 in NAT mode.

  NOTE

  A device out of the cluster accesses the FTP server in the cluster in NAT mode. IP address of the FTP server is that of the management VLANIF interface on the administrator switch. The FTP server uses a port number reserved in the cluster instead of the commonly-used 21.

```
ftp> open 1.0.0.1 53252
Connected to 1.0.0.1.
220 FTP service ready.
User (1.0.0.1:(none)): hgmp
331 Password required for hgmp.
Password:
230 User logged in.
ftp>
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
```

```
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 FTP server enable
#
```

```
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

9.3.3 Example for Configuring the Interconnection of FTP Servers and Devices in and out of the HGMP Cluster (in Non-NAT Mode)

Networking Requirements

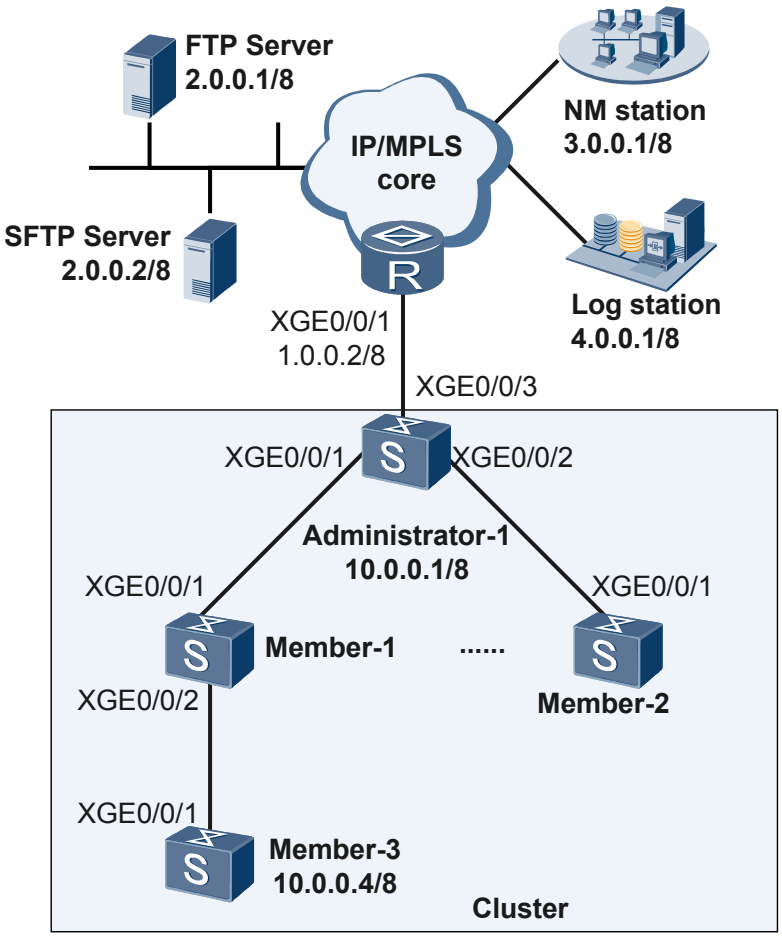
As shown in **Figure 9-9**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

To upload files to Member-1, Member-2, and Member-3 or download files from them, you can set up an FTP connection between devices out of the cluster and member switches in NAT or non-NAT mode.

NOTE

In this configuration example where the Non-NAT mode is adopted, Member-3 accesses the FTP server (2.0.0.1/8) out of the cluster and devices out of the cluster access the FTP server (Member-2) in the cluster.

Figure 9-9 Networking diagram of configuring the interconnection of FTP servers and devices in and out of the HGMP cluster (in non-NAT mode)



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster and configure basic HGMP functions for the cluster according to the steps described in the section **Example for Configuring Basic HGMP Functions for a Cluster**.
2. Disable FTP NAT on the administrator switch (The function is disabled by default.)

   NOTE

   Related configurations of cluster NAT must be performed on the administrator switch.
3. Configure routes on the administrator switch and member switches to ensure that reachable routes exist between the FTP server and member switches.
4. For the situation that Member-3 accesses the FTP server (2.0.0.1/8) out of the cluster:

- Run the **ftp** command on the member switch to set up a connection with the public FTP server of the cluster.

5. For the situation that the device out of the cluster accesses the FTP server (Member-2):
   - Run the FTP client program on the PC and create an FTP connection with the member switch.

Context

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the FTP server
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8
- Member ID serving as the FTP server in the cluster with the member ID being 2

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
```

```
Interface: XGigabitEthernet0/0/1
   Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
   Neighbor 1:  Aging Time: 2(s)
      MAC Address : 0002-0002-0002
      Port Name   : XGigabitEthernet0/0/1
      Software Version: Version 5.70 V200R006C00
      Device Name : Member-1
      Port Duplex : FULL
      Product Ver : S6700
Interface: XGigabitEthernet0/0/2
   Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
   Neighbor 1:  Aging Time: 5(s)
      MAC Address : 0003-0003-0003
      Port Name   : XGigabitEthernet0/0/1
      Software Version: Version 5.70 V200R006C00
      Device Name : Member-2
      Port Duplex : FULL
      Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
```

```
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                           Hop   MAC Address     DeviceType
Member-1                       1     0002-0002-0002   S6700
Member-2                       1     0003-0003-0003   S6700
Member-3                       2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
-------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure routes for the member switches and ensure that reachable routes exist between member switches and the FTP server.

Configure member switch 1.

```
[HUAWEI_1.Member-1] ip route-static 2.0.0.0 8 10.0.0.1
```

Configure member switch 2.

```
[HUAWEI_2.Member-2] ip route-static 2.0.0.0 8 10.0.0.1
```

Configure member switch 3.

```
[HUAWEI_3.Member-3] ip route-static 2.0.0.0 8 10.0.0.1
```

NOTE

Multiple member switches can be configured simultaneously through incremental configuration. For configuration details, see **Example for Configuring the Incremental Configuration Function for an HGMP Cluster**.

Step 10 Verify the configuration.

- Member switches access the FTP server in non-NAT mode.

```
< HUAWEI_3.Member-3> ftp 2.0.0.1
Trying 2.0.0.1 ...
Press CTRL+K to abort
Connected to 2.0.0.1.
220 FTP service ready.
User(2.0.0.1:(none)):hgmp
331 Password required for hgmp.
Enter password:
```

```
230 User logged in.
[ftp]
```

- Devices out of the cluster access the FTP server in the cluster in non-NAT mode.

  # Configure an FTP server on the corresponding member switch (Member-2). The configuration details see Configuration Files, and are not mentioned here.

  # Run the FTP client program on the PC and set up an FTP connection with Member-2 in non-NAT mode.

  NOTE

  Devices out of the cluster access the FTP server in the cluster in non-NAT mode. The IP address of the FTP server is that of the management VLANIF interface on the member switch. The FTP server uses a port number reserved in the cluster instead of the commonly-used 21.

```
ftp> open 10.0.0.2
Connected to 10.0.0.2
220 FTP service ready.
User (10.0.0.2:(none)): hgmp
331 Password required for hgmp.
Password:
230 User logged in.
ftp>
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 administrator-address 0001-0001-0001 name HUAWEI
#
 mngvlanid 10
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
```

```
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 administrator-address 0001-0001-0001 name HUAWEI
#
 mngvlanid 10
 ip route-static 2.0.0.0 255.0.0.0 10.0.0.1
#
return
```

9.3.4 Example for Configuring Devices in the HGMP Cluster to Access the Outside SNMP Host (in NAT Mode)

Networking Requirements

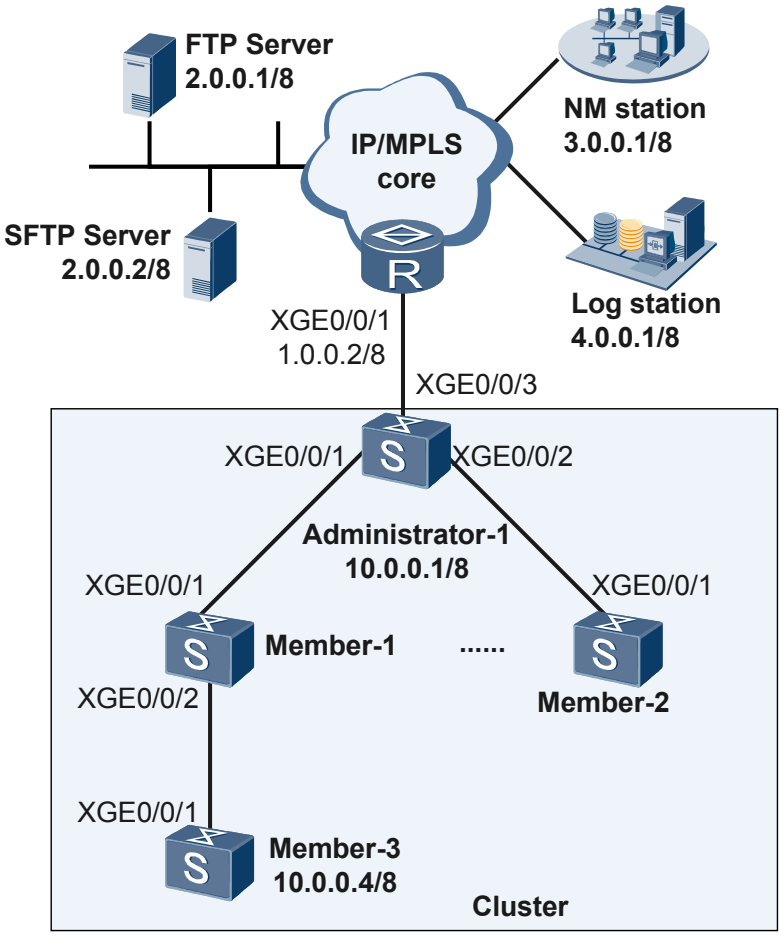
As shown in **Figure 9-10**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

When Member-1, Member-2, and Member-3 are required to send packets to the SNMP host, a connection can be set up between the SNMP host out of the cluster and member switches in NAT or non-NAT mode.

NOTE

In this configuration example where the NAT mode is adopted, Member-3 accesses the outside SNMP host (3.0.0.1/8).

Figure 9-10 Networking diagram of configuring devices in the HGMP cluster to access the outside SNMP host (in NAT mode)



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster and configure basic HGMP functions for the cluster according to the steps described in **Example for Configuring Basic HGMP Functions for a Cluster**.
2. Enable SNMP NAT on the administrator switch (The function is enabled by default.)

   NOTE

   Related configurations of cluster NAT must be performed on the administrator switch.
3. Assign an IP address to the SNMP host.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of the SNMP host, that is 3.0.0.1/8
- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the SNMP host
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
```

```
MAC Address : 0003-0003-0003
Port Name   : XGigabitEthernet0/0/1
Software Version: Version 5.70 V200R006C00
Device Name : Member-2
Port Duplex : FULL
Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
```

```
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                            Hop   MAC Address     DeviceType
Member-1                        1     0002-0002-0002   S6700
Member-2                        1     0003-0003-0003   S6700
Member-3                        2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-------------------------------------------------------------------------------
SN   Device Type             MAC Address     Status Device Name
-------------------------------------------------------------------------------
0    S6700                   0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                   0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                   0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                   0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
```

```
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

9.3.5 Example for Configuring Devices in the HGMP Cluster to Access the Outside SNMP Host (in non-NAT Mode)

Networking Requirements

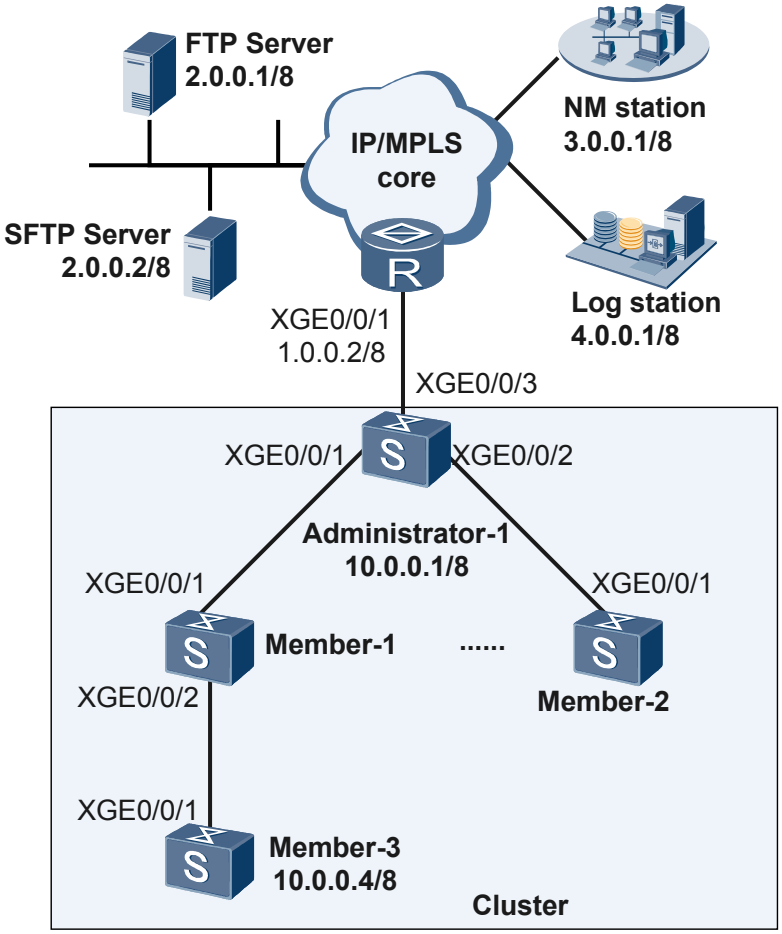
As shown in **Figure 9-11**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

When Member-1, Member-2, and Member-3 are required to send packets to the SNMP host out of the cluster, a connection can be set up between the SNMP host and member switches in NAT or non-NAT mode.

NOTE

In this configuration example where the non-NAT mode is adopted, Member-3 accesses the SNMP host (3.0.0.1/8).

Figure 9-11 Networking diagram of configuring devices in the HGMP cluster to access the outside SNMP host (in non-NAT mode)



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster and configure basic HGMP functions for the cluster according to the steps described in **Example for Configuring Basic HGMP Functions for a Cluster**.
2. Disable SNMP NAT on the administrator switch (The function is enabled by default.)

   NOTE

   Related configurations of cluster NAT must be performed on the administrator switch.
3. Configure routes on the administrator switch and member switches respectively to ensure that reachable routes exist between SNMP host and member switches.
4. Assign an IP address to the SNMP host.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of the SNMP host, that is 3.0.0.1/8
- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the SNMP host
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
```

```
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

--------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   S6700
Member-2                      1     0003-0003-0003   S6700
Member-3                      2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
--------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
--------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Disable SNMP NAT on the administrator switch.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-snmp-nat enable
```

Step 11 Configure the routes of member switches to ensure that reachable routes exist between member switches and the SNMP host.

Configure member switch 1.

```
[HUAWEI_1.Member-1] ip route-static 3.0.0.0 8 10.0.0.1
```

Configure member switch 2.

```
[HUAWEI_2.Member-2] ip route-static 3.0.0.0 8 10.0.0.1
```

Configure member switch 3.

```
[HUAWEI_3.Member-3] ip route-static 3.0.0.0 8 10.0.0.1
```

NOTE

Multiple member switches can be configured simultaneously through incremental configuration. For configuration details, see **Example for Configuring the Incremental Configuration Function for an HGMP Cluster**.

Step 12 Configure the SNMP agent function on member switches.

Configure member switch 1.

```
[HUAWEI_1.Member-1] snmp-agent target-host trap address udp-domain 3.0.0.1 params
securityname cluster
```

Configure member switch 2.

```
[HUAWEI_2.Member-2] snmp-agent target-host trap address udp-domain 3.0.0.1 params
securityname cluster
```

Configure member switch 3.

```
[HUAWEI_3.Member-3] snmp-agent target-host trap address udp-domain 3.0.0.1 params
securityname cluster
```

NOTE

Multiple member switches can be configured simultaneously through incremental configuration. For configuration details, see **Example for Configuring the Incremental Configuration Function for an HGMP Cluster**.

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 undo cluster-snmp-nat enable
       cluster-ftp-nat enable
       ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
```

```
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
 snmp-agent
 snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname
cluster
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
 snmp-agent
 snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname
cluster
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
```

```
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
 ip route-static 3.0.0.0 255.0.0.0 10.0.0.1
#
 snmp-agent
 snmp-agent target-host trap address udp-domain 3.0.0.1 params securityname
cluster
#
return
```

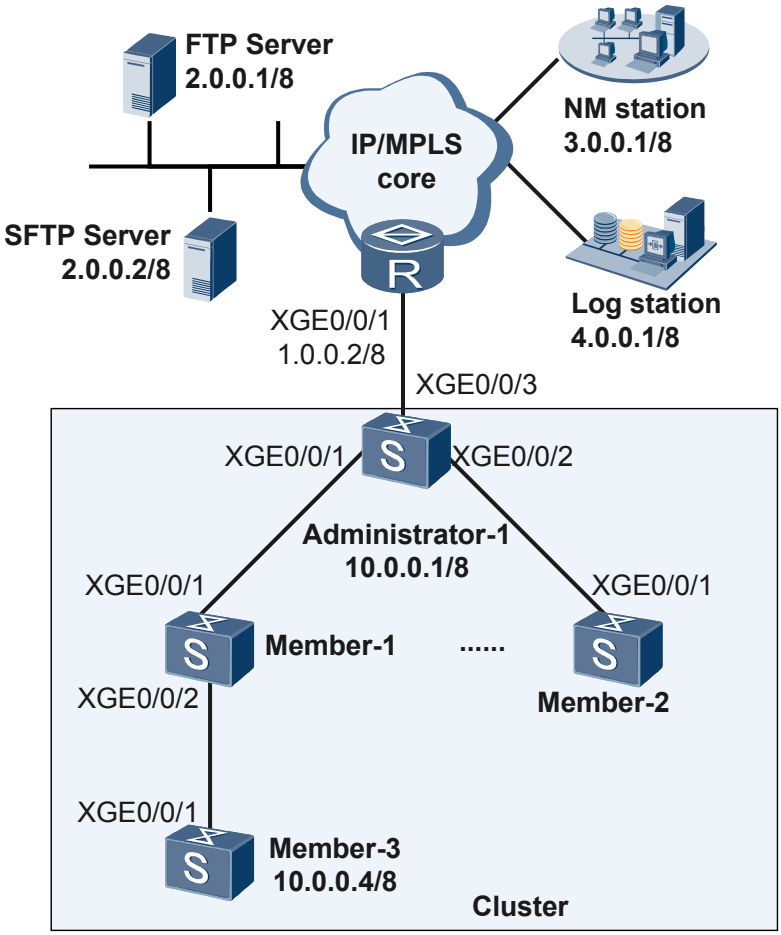
9.3.6 Example for Configuring the Batch Distribution Function for an HGMP Cluster

Networking Requirements

As shown in **Figure 9-12**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

Member-2 and Member-3 are required to download configuration files in batches from the FTP server.

Figure 9-12 Networking diagram of configuring the batch distribution function for an HGMP cluster



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster according to the steps described in **9.3.1 Example for Configuring Basic HGMP Functions for a Cluster**.
2. **9.3.1 Example for Configuring Basic HGMP Functions for a Cluster**

   NOTE

   - Configure the interconnection of FTP servers and devices in and out of the HGMP cluster in NAT or non-NAT mode. The following takes the configuration in NAT mode as an example.
   - If the system software, patch files, or configuration files, batch distribution can be distributed in batches without accessing the FTP server out of the cluster, you can skip this step.
3. Configure batch distribution on the administrator switch.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the FTP server
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8
- Member ID of Member-2 being 2 and member ID of Member-3 being 3

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
```

```
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
```

```
      Port Duplex : FULL
      Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
      MAC Address : 0003-0003-0003
      Port Name   : XGigabitEthernet0/0/1
      Software Version: Version 5.70 V200R006C00
      Device Name : Member-2
      Port Duplex : FULL
      Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
```

```
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                           Hop   MAC Address     DeviceType
Member-1                       1     0002-0002-0002   S6700
Member-2                       1     0003-0003-0003   S6700
Member-3                       2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
```

```
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Distribute configuration files in batches.

Run the batch distribution command on the administrator switch. Member switches download configuration files from the FTP server (2.0.0.1) in NAT mode and automatically set them as the default configuration files for the next startup.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plug-play ip 2.0.0.1 username user1
password 123
[HUAWEI_0.Administrator-1-cluster] cluster-member group-by member-number 2 to 3
get configuration-file vrpcfg-hgmp.zip
```

Step 11 Verify the configuration.

Run the **display member-getfile-stat** command on the administrator switch to check whether member switches successfully obtain the configuration files, system software, and patch files, and you can view that **success** is displayed.

```
[HUAWEI_0.Administrator-1] display member-getfile-stat
The status of member switchs getting file:
--------------------------------------------------------------------------
SN    Device              MacAddress        IPAddress        Result
--------------------------------------------------------------------------
2     S6700               0003-0003-0003    10.0.0.3         success
3     S6700               0004-0004-0004    10.0.0.4         success
```

Run the **dir** command on member switches and you can find that member switches successfully download the specified configuration files. Take Member-2 as an example.

```
<HUAWEI_2.Member-2> dir *.zip
Directory of flash:/
  Idx  Attr  Size(Byte)  Date        Time       FileName
   0   -rw-       1,491  Sep 03 2008 17:43:52   vrpcfg.zip
   1   -rw-         752  Aug 05 2008 15:04:36   vrpcfg-hgmp.zip
506,880 KB total (35,920 KB free)
```

Run the **display startup** command on member switches and you can find that names of the configuration files for the next startup of the member switch is changed. Take Member-2 as an example.

```
<HUAWEI_2.Member-2> display startup
MainBoard:
  Configured startup system software:        flash:/S6700.cc
  Startup system software:                   flash:/S6700.cc
  Next startup system software:              flash:/S6700.cc
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg-hgmp.zip
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     NULL
  Next startup patch package:                NULL
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
```

```
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

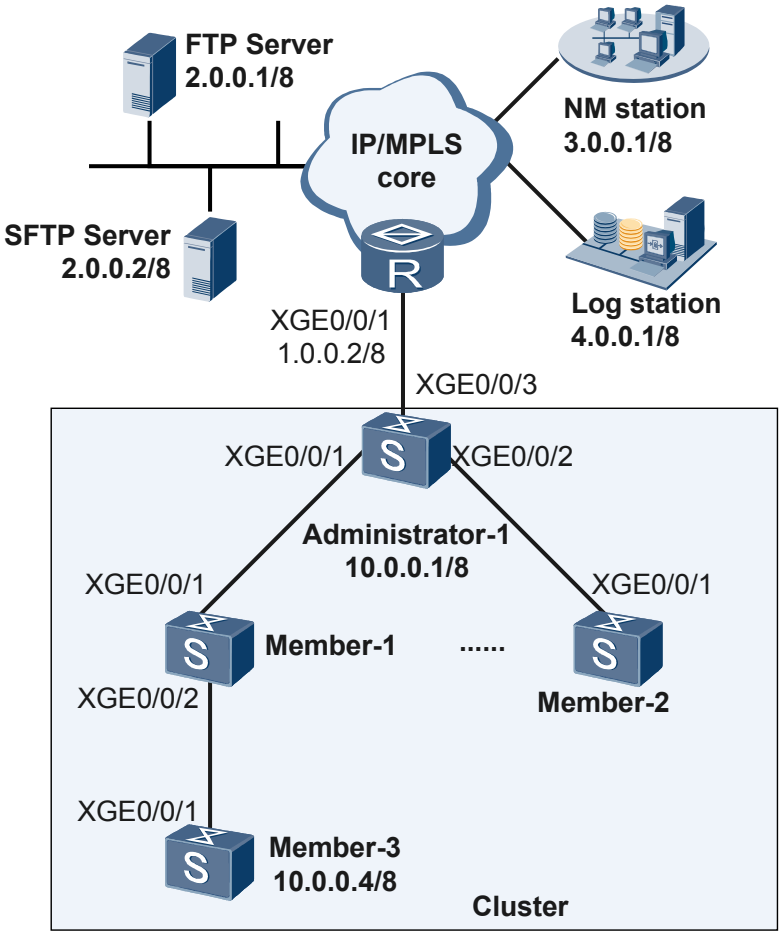
9.3.7 Example for Configuring the Batch Restart Function for an HGMP Cluster

Networking Requirements

As shown in **Figure 9-13**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

Member switches Member-2 and Member-3 are required to be restarted.

Figure 9-13 Networking diagram of configuring the batch restart function for an HGMP cluster



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster according to the steps described in **9.3.1 Example for Configuring Basic HGMP Functions for a Cluster**.
2. Configure batch restart on the administrator switch.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of VLANIF 10, that is 1.0.0.1/8
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8
- Member ID of Member-2 being 2 and the member ID of Member-3 being 3

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
```

```
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
       Port Duplex : FULL
```

```
      Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-2
       Port Duplex : FULL
       Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
```

```
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                           Hop   MAC Address     DeviceType
Member-1                       1     0002-0002-0002   S6700
Member-2                       1     0003-0003-0003   S6700
Member-3                       2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
```

```
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Restart member switches in batches.

Run the **cluster-member reboot group-by member-number 2 to 3** command on the administrator switch to restart Member-2 and Member-3.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-member reboot group-by member-number 2
to 3
Info: This command will take members reboot.
Are you sure?[Y/N]y
```

Step 11 Verify the configuration.

Run the **display member-reboot-stat** command on administrator switch to check the restart status of the member switches, and you can view that **success** is displayed, which indicates that the specified member switches are restarted successfully.

```
[HUAWEI_2.Member-2] display member-reboot-stat
The result of member switchs rebooting:
------------------------------------------------------------------------------
SN    Device              MacAddress        IPAddress        Result
------------------------------------------------------------------------------
1     S6700               0003-0003-0003    10.0.0.3         success
2     S6700               0004-0004-0004    10.0.0.4         success
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
```

```
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
```

```
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

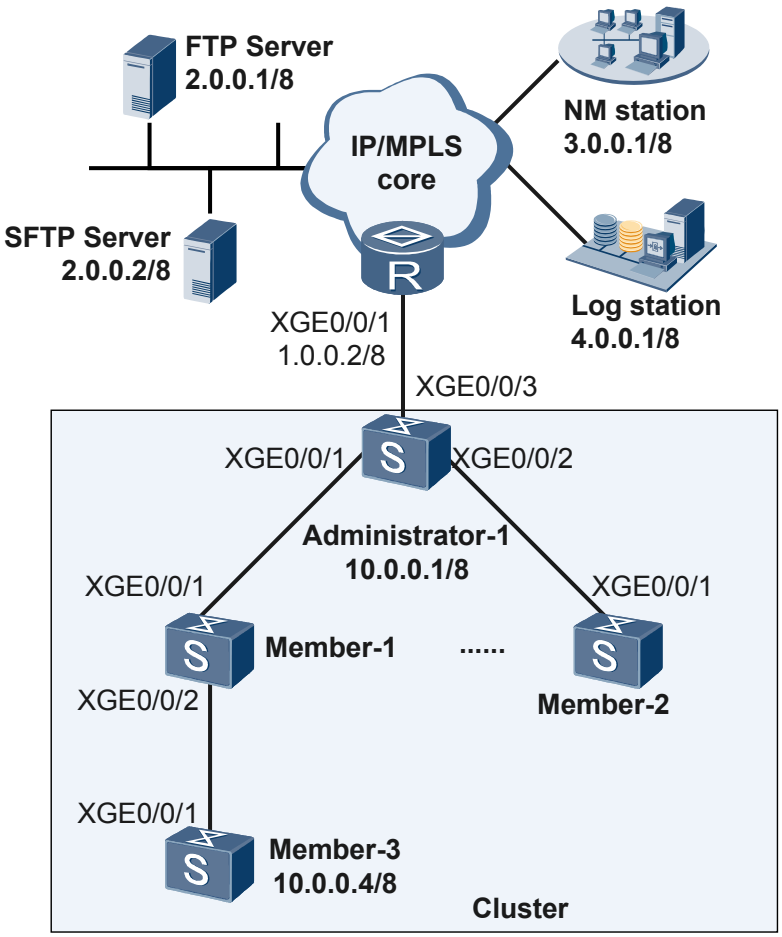
9.3.8 Example for Configuring the Incremental Configuration Function for an HGMP Cluster

Networking Requirements

As shown in **Figure 9-14**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

To configure VLAN 100 to VLAN 200 on Member-2 and Member-3 and a static route with its next hop address being the administrator switch, you can use the incremental configuration function of the HGMP cluster.

Figure 9-14 Networking diagram of configuring the incremental configuration function for an HGMP cluster



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster according to the steps described in **9.3.1 Example for Configuring Basic HGMP Functions for a Cluster**.
2. Edit the list of incremental configurations command on the administrator switch.
3. Deliver the list of incremental configuration commands to the specified member switch.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10

- IP address of VLANIF 10, that is 1.0.0.1/8
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8
- Member ID of Member-2 being 2 and the member ID of Member-3 being 3

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
```

```
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
```

```
Device Name : Member-2
Port Duplex : FULL
Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
```

```
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join     : disabled
Handshake timer:10 sec
```

```
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   S6700
Member-2                      1     0003-0003-0003   S6700
Member-3                      2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
-------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Edit the list of incremental configuration commands on the administrator switch.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] increment
[HUAWEI_0.Administrator-1-cluster-increment] increment-command command-number 10
command-text vlan batch 100 to 200
```

```
[HUAWEI_0.Administrator-1-cluster-increment] increment-command command-number 20
command-text ip route-static 2.0.0.0 8 10.0.0.1
```

After the previous configuration, run the **display increment-command** command on the administrator switch to check the list of incremental configuration commands.

```
[HUAWEI_0.Administrator-1] display increment-command
The content of increment commands:
-------------------------------------------------------------------------------
SN        Content
-------------------------------------------------------------------------------
10        vlan batch 100 to 200
20        ip route-static 2.0.0.0 8 10.0.0.1
```

Step 11 Deliver the list of incremental configurations command to the specified member switch.

```
[HUAWEI_0.Administrator-1-cluster-increment] increment-run group-by member-number
2 to 3
```

Step 12 Verify the configuration.

Run the **display cluster-increment-result** command on administrator switch to check whether the list of incremental configuration commands is delivered to the specified member switch, and you can view that **success** is displayed.

```
[HUAWEI_0.Administrator-1] display cluster-increment-result
The result of member switch executing increment commands:
-------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      Result    CommandId
-------------------------------------------------------------------------------
2    S6700               0003-0003-0003 10.0.0.3       success   -

3    S6700               0004-0004-0004 10.0.0.4       success   -
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
```

```
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
```

```
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

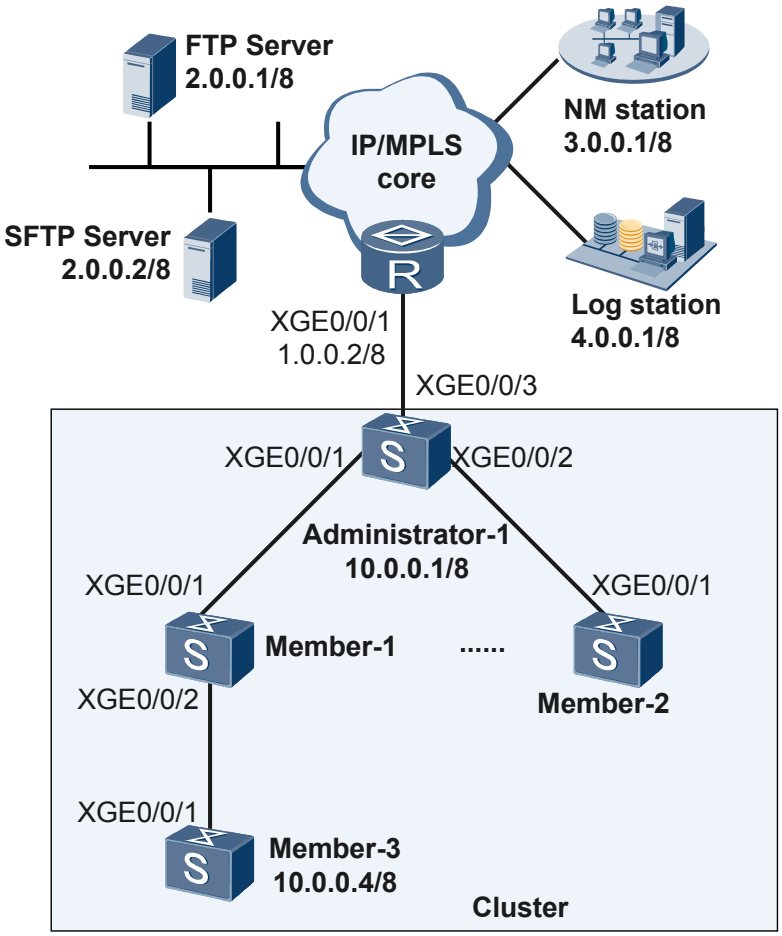
9.3.9 Example for Configuring the Configuration Synchronization Function for an HGMP Cluster

Networking Requirements

As shown in **Figure 9-15**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

To synchronize the configuration files of all member switches to the FTP server as required, you can configure the configuration synchronization function for the HGMP cluster.

Figure 9-15 Networking diagram of configuring the configuration synchronization function for an HGMP cluster



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster according to the steps described in **9.3.1 Example for Configuring Basic HGMP Functions for a Cluster**.
2. **9.3.2 Example for Configuring the Interconnection of FTP Servers and Devices in and out of the HGMP Cluster (in NAT Mode)**

   NOTE

   - Configure the interconnection of FTP servers and devices in and out of the HGMP cluster in NAT or non-NAT mode. The following takes the configuration in NAT mode as an example.
   - If it is not required to synchronize the configuration files of the HGMP cluster by accessing the FTP server out of the cluster, you can skip this step.

3. Run the configuration synchronization command on the administrator switch.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10
- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the FTP server
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
```

```
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
```

```
      Device Name : Member-1
      Port Duplex : FULL
      Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
      MAC Address : 0003-0003-0003
      Port Name   : XGigabitEthernet0/0/1
      Software Version: Version 5.70 V200R006C00
      Device Name : Member-2
      Port Duplex : FULL
      Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
```

```
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                  PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                        S6700
 0003-0003-0003  1                        S6700
 0002-0002-0002  1                        S6700
 0001-0001-0001  0                        S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                            Hop   MAC Address     DeviceType
Member-1                        1     0002-0002-0002   S6700
Member-2                        1     0003-0003-0003   S6700
Member-3                        2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
```

```
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Synchronize configuration files.

Run the configuration synchronization command on the administrator switch, and then member switches synchronize configuration files to the FTP server (2.0.0.1) in NAT mode.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plug-play ip 2.0.0.1 username hgmp
password hgmp
[HUAWEI_0.Administrator-1-cluster] increment-config synchronization
```

Step 11 Verify the configuration.

After the previous configuration, run the **display increment-synchronization-result** command on administrator switch to check whether configuration files are synchronized to the FTP server, and you can view that **success** is displayed.

```
[HUAWEi_0.Administrator-1] display increment-synchronization-result
The result of member switchs' synchronization:
-------------------------------------------------------------------------------
SN   Device              MacAddress     IpAddress      result
-------------------------------------------------------------------------------
1    S6700               0002-0002-0002 10.0.0.2       success
2    S6700               0003-0003-0003 10.0.0.3       success
3    S6700               0004-0004-0004 10.0.0.4       success
```

On the FTP server, you can view that the names of configuration files are the MAC address of member switches, which indicates that configuration synchronization is successful.

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
```

```
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp-server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 FTP server enable
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
```

```
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 5
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

9.3.10 Example for Configuring Security Features for an HGMP Cluster

Networking Requirements

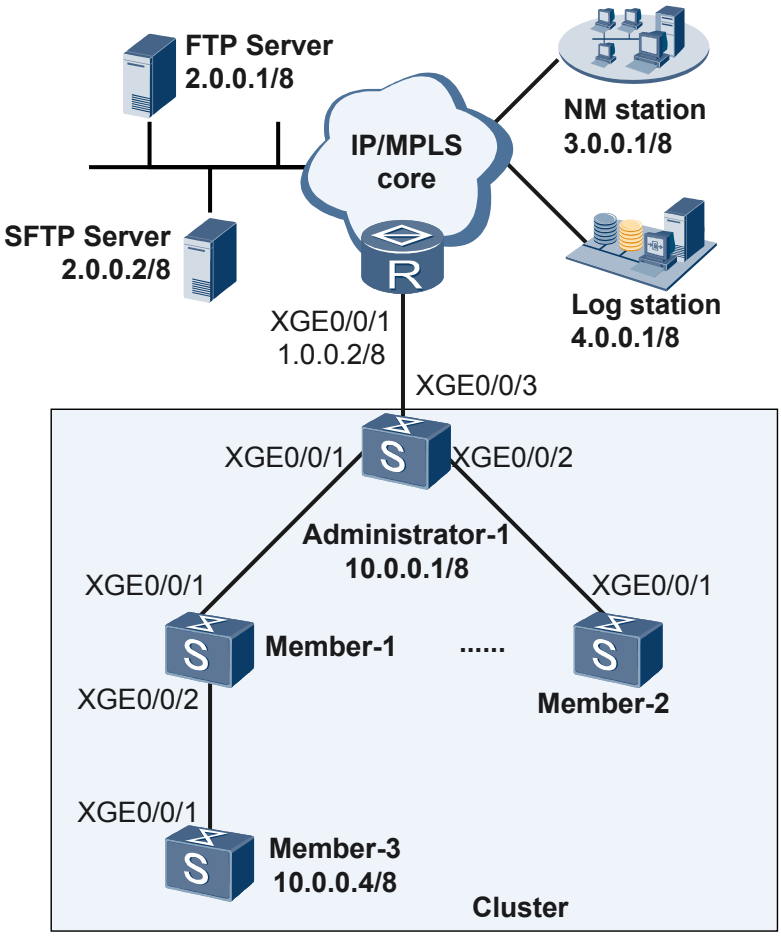
As shown in **Figure 9-16**, all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

Disable NDP and NTDP on the interfaces of all the member switches that do not need NDP or NTDP. To perform the action and improve the security of the cluster, you can configure security features for the HGMP cluster.

NOTE

After NDP or NTDP is disabled on unrelated interfaces of member switches, if the new candidate switches are connected to these unrelated interfaces, they cannot join the cluster until NDP or NTDP is enabled.

Figure 9-16 Networking diagram of configuring security features for an HGMP cluster



Device	MAC Address	Device	MAC Address
Administrator-1	0001-0001-0001	Member-1	0002-0002-0002
Member-2	0003-0003-0003	Member-3	0004-0004-0004

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster according to the steps described in **9.3.1 Example for Configuring Basic HGMP Functions for a Cluster**.
2. On the administrator switch, disable NDP and NTDP on unrelated interfaces of member switches.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 10

- IP address of VLANIF 10 that is 1.0.0.1/8 and a reachable route between VLANIF 10 and the FTP server
- Address pool of the cluster, that is 10.0.0.0/8
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8

Procedure

Step 1 Configure a management VLAN.

Create VLAN 10 on the device and add interfaces of the administrator switch and member switches to VLAN 10.

Configure the administrator switch.

```
<Quidway> system-view
[Quidway] sysname Administrator-1
[Administrator-1] vlan 10
[Administrator-1-vlan10] quit
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/2] quit
[Administrator-1] interface xgigabitethernet 0/0/3
[Administrator-1-XGigabitEthernet0/0/3] port link-type trunk
[Administrator-1-XGigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Administrator-1-XGigabitEthernet0/0/3] quit
[Administrator-1] interface vlanif 10
[Administrator-1-Vlanif10] quit
```

Configure member switch 1.

```
<Quidway> system-view
[Quidway] sysname Member-1
[Member-1] vlan 10
[Member-1-vlan10] quit
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] port link-type trunk
[Member-1-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] port link-type trunk
[Member-1-XGigabitEthernet0/0/2] port trunk allow-pass vlan 10
[Member-1-XGigabitEthernet0/0/2] quit
[Member-1] interface vlanif 10
[Member-1-Vlanif10] quit
```

Configure member switch 2.

```
<Quidway> system-view
[Quidway] sysname Member-2
[Member-2] vlan 10
[Member-2-vlan10] quit
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] port link-type trunk
[Member-2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-2-XGigabitEthernet0/0/1] quit
[Member-2] interface vlanif 10
[Member-2-Vlanif10] quit
```

Configure member switch 3.

```
<Quidway> system-view
```

```
[Quidway] sysname Member-3
[Member-3] vlan 10
[Member-3-vlan10] quit
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] port link-type trunk
[Member-3-XGigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Member-3-XGigabitEthernet0/0/1] quit
[Member-3] interface vlanif 10
[Member-3-Vlanif10] quit
```

Step 2 Configure NDP.

On switches, enable NDP in the system view and on an interface.

Configure the administrator switch.

```
[Administrator-1] ndp enable
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ndp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ndp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ndp enable
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ndp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ndp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ndp enable
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ndp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ndp enable
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ndp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, you can find that NDP on the administrator is in the Enable state, the host name of the neighboring node is Device Name, and the name of the interface connecting the neighboring node and the local interface is Port Name.

```
[Administrator-1] display ndp interface xgigabitethernet 0/0/1 xgigabitethernet
0/0/2
 Interface: XGigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 0, Packets Received: 11, Packets Error: 0
    Neighbor 1:  Aging Time: 2(s)
       MAC Address : 0002-0002-0002
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
       Device Name : Member-1
       Port Duplex : FULL
       Product Ver : S6700
 Interface: XGigabitEthernet0/0/2
    Status: Enabled, Packets Sent: 6, Packets Received: 16, Packets Error: 0
    Neighbor 1:  Aging Time: 5(s)
       MAC Address : 0003-0003-0003
       Port Name   : XGigabitEthernet0/0/1
       Software Version: Version 5.70 V200R006C00
```

```
Device Name : Member-2
Port Duplex : FULL
Product Ver : S6700
```

Step 3 Configure NTDP.

On devices, enable NTDP in the system view and on the interface and configure the interval and range for NTDP to collect topologies to 10 minutes and 3 hops respectively.

Configure the administrator switch.

```
[Administrator-1] ntdp enable
[Administrator-1] ntdp timer 10
[Administrator-1] ntdp hop 3
[Administrator-1] interface xgigabitethernet 0/0/1
[Administrator-1-XGigabitEthernet0/0/1] ntdp enable
[Administrator-1-XGigabitEthernet0/0/1] quit
[Administrator-1] interface xgigabitethernet 0/0/2
[Administrator-1-XGigabitEthernet0/0/2] ntdp enable
[Administrator-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 1.

```
[Member-1] ntdp enable
[Member-1] ntdp timer 10
[Member-1] ntdp hop 3
[Member-1] interface xgigabitethernet 0/0/1
[Member-1-XGigabitEthernet0/0/1] ntdp enable
[Member-1-XGigabitEthernet0/0/1] quit
[Member-1] interface xgigabitethernet 0/0/2
[Member-1-XGigabitEthernet0/0/2] ntdp enable
[Member-1-XGigabitEthernet0/0/2] quit
```

Configure member switch 2.

```
[Member-2] ntdp enable
[Member-2] ntdp timer 10
[Member-2] ntdp hop 3
[Member-2] interface xgigabitethernet 0/0/1
[Member-2-XGigabitEthernet0/0/1] ntdp enable
[Member-2-XGigabitEthernet0/0/1] quit
```

Configure member switch 3.

```
[Member-3] ntdp enable
[Member-3] ntdp timer 10
[Member-3] ntdp hop 3
[Member-3] interface xgigabitethernet 0/0/1
[Member-3-XGigabitEthernet0/0/1] ntdp enable
[Member-3-XGigabitEthernet0/0/1] quit
```

After the previous configuration, globally check the NTDP configuration on the administrator switch. You can find that the interval and range for NTDP to collect topologies is 10 minutes and 3 hops respectively.

```
[Administrator-1] display ntdp
Network topology discovery protocol is enabled
Hops      : 3
Timer     : 10 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection:0 ms
```

Step 4 Enable the cluster function and set the management VLAN.

Configure the administrator switch.

```
[Administrator-1] cluster enable
[Administrator-1] cluster
```

```
[Administrator-1-cluster] mngvlanid 10
[Administrator-1-cluster] quit
```

Configure member switch 1.

```
[Member-1] cluster enable
[Member-1] cluster
[Member-1-cluster] mngvlanid 10
[Member-1-cluster] quit
```

Configure member switch 2.

```
[Member-2] cluster enable
[Member-2] cluster
[Member-2-cluster] mngvlanid 10
[Member-2-cluster] quit
```

Configure member switch 3.

```
[Member-3] cluster enable
[Member-3] cluster
[Member-3-cluster] mngvlanid 10
[Member-3-cluster] quit
```

After the topology collection function is enabled manually on the administrator switch, check the device information collected through NTDP and you can find the MAC address and types of related devices.

```
<Administrator-1> ntdp explore
<Administrator-1> system-view
[Administrator-1] display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC             HOP  IP                 PLATFORM

------------------------------------------------------------------------------
 0004-0004-0004  2                       S6700
 0003-0003-0003  1                       S6700
 0002-0002-0002  1                       S6700
 0001-0001-0001  0                       S6700
```

Step 5 Create a cluster.

NOTE

Following steps can be performed only on the administrator switch.

On the administrator switch, set the range of IP addresses that can be assigned to the cluster to 10.0.0.0/8, in which the IP address assigned to the administrator switch is 10.0.0.1/8.

```
[Administrator-1] cluster
[Administrator-1-cluster] ip-pool 10.0.0.1 8
```

Create a cluster named HUAWEI on the administrator switch.

```
[Administrator-1-cluster] build HUAWEI
[HUAWEI_0.Administrator-1-cluster]
```

After the previous configuration, check information about the cluster to which the device belongs. You can find that the device name is changed, the cluster name is HUAWEI, and the management VLAN ID is 10.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join     : disabled
Handshake timer:10 sec
```

```
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
No logging host configured
No SNMP host configured
No FTP server configured
No SFTP server configured
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 1 member(s) in the cluster, and 0 of them are down.
```

On the administrator switch, check information about candidate switches, you can find all the candidate switches and their types.

```
[HUAWEI_0.Administrator-1-cluster] display cluster candidates
MAC             HOP  IP                  PLATFORM
0004-0004-0004  2                        S6700
0003-0003-0003  1                        S6700
0002-0002-0002  1                        S6700
```

Step 6 Add member switches.

NOTE

- Following steps can be performed only on the administrator switch.
- Take the mode of automatically adding member switches as an example. To add member switches manually, see Adding a Member Switch.

Add all candidate switches to the cluster.

```
[HUAWEI_0.Administrator-1-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name                          Hop   MAC Address     DeviceType
Member-1                      1     0002-0002-0002   S6700
Member-2                      1     0003-0003-0003   S6700
Member-3                      2     0004-0004-0004   S6700
Warning: Add all to cluster?(Y/N) y
Info: Cluster auto-build is complete.
Added 3 member(s) into the cluster successfully.
```

After the previous configuration, check information about the administrator switch and member switches in the cluster on the administrator switch. You can find that all the member switches are added to the cluster and in the Up state.

```
[HUAWEI_0.Administrator-1-cluster] display cluster members
The list of cluster member:
-------------------------------------------------------------------------------
SN   Device Type              MAC Address     Status Device Name
-------------------------------------------------------------------------------
0    S6700                    0001-0001-0001  Admin  HUAWEI_0.Administrator-1
1    S6700                    0002-0002-0002  Up     HUAWEI_1.Member-1
2    S6700                    0003-0003-0003  Up     HUAWEI_2.Member-2
3    S6700                    0004-0004-0004  Up     HUAWEI_3.Member-3
```

Step 7 Assign an IP address to VLANIF 10.

To ensure the normal communication between member switches in the cluster and devices out of the cluster, assign an IP address to VLANIF 10 on the administrator switch.

Assign an IP address to VLANIF 10.

```
[HUAWEI_0.Administrator-1] interface vlanif 10
[HUAWEI_0.Administrator-1-Vlanif10] ip address 1.0.0.1 8
[HUAWEI_0.Administrator-1-Vlanif10] quit
```

After the previous configuration, you can find that the interface on the administrator switch is in the Up state.

```
[HUAWEI_0.Administrator-1] display interface Vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Vlanif10 Interface
Route Port,The MTU is 1500
Internet Address is 1.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0001-0001-0001
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 8 Configure a static route on the administrator switch.

This operation is to ensure that a reachable route exists between switches in the cluster and servers or hosts.

```
[HUAWEI_0.Administrator-1] ip route-static 0.0.0.0 0 1.0.0.2
```

NOTE

You can also run a routing protocol.

Step 9 Configure public servers and hosts of the cluster.

Configure an FTP server.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-ftp-nat enable
[HUAWEI_0.Administrator-1-cluster] ftp-server 2.0.0.1
```

Configure a SFTP server.

```
[HUAWEI_0.Administrator-1-cluster] sftp-server 2.0.0.2
```

Configure a Simple Network Management Protocol (SNMP) host.

```
[HUAWEI_0.Administrator-1-cluster] snmp-host 3.0.0.1
```

Configure a log host.

```
[HUAWEI_0.Administrator-1-cluster] logging-host 4.0.0.1
```

After the previous configuration, check information about the cluster to which the administrator switch belongs. You can find that the public log host, SNMP host, FTP server, and SFTP server are configured successfully.

```
[HUAWEI_0.Administrator-1-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch
management vlan id    : 10
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join      : disabled
Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
SFTP server:2.0.0.2
cluster-member ftp-timeout: 300 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : enabled
There are 4 member(s) in the cluster, and 0 of them are down.
```

Step 10 Disable NDP and NTDP.

Disable NDP and NTDP on interfaces of all the member switches that do not need NDP and NTDP.

```
# Disable NDP on the unrelated interfaces of member switches
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ndp
# Disable NTDP on the unrelated interfaces of member switches
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ntdp
```

Step 11 Verify the configuration.

After the previous configuration, run the **display member-interface-state** command on administrator switch to check whether NDP or NTDP is disabled on unrelated interfaces of the member switches, and you can view that **success** is displayed.

```
[HUAWEI_0.Administrator-1] display member-interface-state ndp
The result of member switches executed disable member interface command:
-------------------------------------------------------------------------------
SN        Device         MacAddress          IpAddress           result
-------------------------------------------------------------------------------
3         S6700          0004-0004-0004      10.0.0.4            success
2         S6700          0003-0003-0003      10.0.0.3            success
1         S6700          0002-0002-0002      10.0.0.2            success
[HUAWEI_0.Administrator-1] display member-interface-state ntdp
The result of member switches executed disable member interface command:
-------------------------------------------------------------------------------
SN        Device         MacAddress          IpAddress           result
-------------------------------------------------------------------------------
3         S6700          0004-0004-0004      10.0.0.4            success
2         S6700          0003-0003-0003      10.0.0.3            success
1         S6700          0002-0002-0002      10.0.0.2            success
```

----End

Configuration Files

- Configuration file of Administrator-1.

```
#
 sysname Administrator-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
 ip address 1.0.0.1 255.0.0.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
cluster
 mngvlanid 10
 ip-pool 10.0.0.1 255.0.0.0
```

```
 build HUAWEI
 cluster-ftp-nat enable
 ftp-server 2.0.0.1
 sftp server 2.0.0.2
 logging-host 4.0.0.1
 snmp-host 3.0.0.1
#
 ip route-static 0.0.0.0 0.0.0.0 1.0.0.2
#
return
```

- Configuration file of Member-1.

```
#
 sysname Member-1
#
 vlan batch 10
#
 cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
interface XGigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-2.

```
#
 sysname Member-2
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

- Configuration file of Member-3.

```
#
 sysname Member-3
#
 vlan batch 10
#
cluster enable
 ntdp enable
 ntdp hop 3
 ntdp timer 10
 ndp enable
#
interface Vlanif10
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 ntdp enable
 ndp enable
#
cluster
 mngvlanid 10
 administrator-address 0001-0001-0001 name HUAWEI
#
return
```

9.4 NTP Configuration

This chapter describes how to configure Network Time Protocol (NTP) to make clocks of the devices on the network identical.

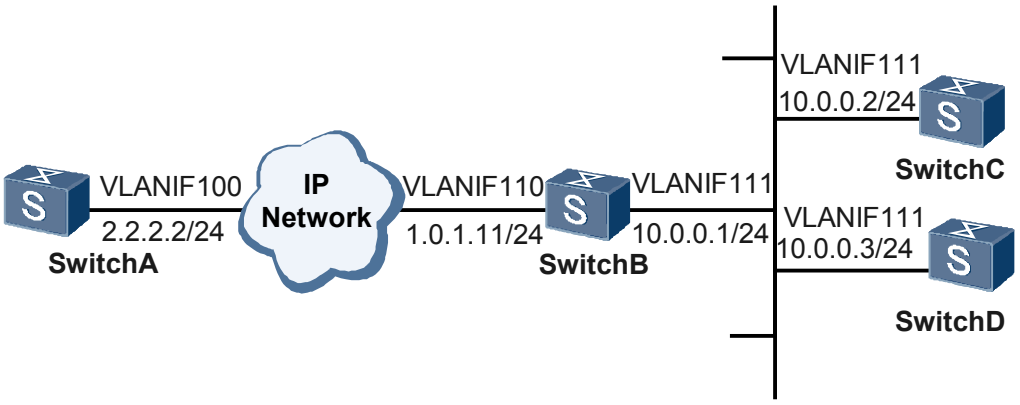
9.4.1 Example for Configuring NTP Authentication in Unicast Client/Server Mode

Networking Requirements

Figure 9-17 shows the diagram of NTP.

- Switch A functions as a unicast NTP server. The clock of Switch A is the master clock with the stratum being 2.
- Switch B functions as a unicast NTP client. Its clock needs to be synchronized with the clock of Switch A.
- Switch C and Switch D function as NTP clients of Switch B.
- NTP authentication needs to be enabled.

Figure 9-17 Networking diagram for configuring the unicast client/server mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch A as an NTP server and configure the master clock on Switch A.
2. Configure Switch B as an NTP client. Switch B synchronizes its clock with the clock of Switch A.
3. Configure Switch C and Switch D to synchronize their clocks with the clock of Switch B.
4. Configure NTP authentication on Switch A, Switch B, Switch C, and Switch D.

   NOTE

   When configuring NTP authentication in unicast client/server mode, pay attention to the following points:

   - You must enable NTP authentication on the client before specifying the IP address of the NTP server and authentication key to be sent to the server; otherwise, NTP authentication is not performed before clock synchronization.
   - To implement authentication successfully, configure both the server and the client.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the reference clock
- Stratum count of the NTP master clock
- Key ID
- Password

Procedure

Step 1 Configure the IP addresses of the Switches and ensure that the routes between them are reachable.

Configure the IP addresses according to **Figure 9-17** so that Switch A, Switch B, Switch C and Switch D are routable.

The configuration procedure is not mentioned.

Step 2 Configure a master NTP clock on Switch A and enable NTP authentication.

On Switch A, set the clock as a master NTP clock with stratum being 2.

```
<SwitchA> system-view
[SwitchA] ntp-service refclock-master 2
```

Enable NTP authentication on Switch A, configure the authentication key, and declare the key to be reliable.

```
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchA] ntp-service reliable authentication-keyid 42
```

The authentication keys configured on the server and the client must be the same.

Step 3 Configure Switch B as the NTP server and enable the NTP authentication.

Enable NTP authentication on Switch B, configure the authentication key, and declare the key to be reliable.

```
<SwitchB> system-view
[SwitchB] ntp-service authentication enable
[SwitchB] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchB] ntp-service reliable authentication-keyid 42
```

Configure Switch A to be the NTP server of Switch B and use the authentication key.

```
[SwitchB] ntp-service unicast-server 2.2.2.2 authentication-keyid 42
```

Step 4 Specify the NTP server for Switch C.

Configure Switch B as the NTP server of Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchC] ntp-service reliable authentication-keyid 42
[SwitchC] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

Step 5 Specify the NTP server for Switch D.

Configure Switch B as the NTP server of Switch D.

```
<SwitchD> system-view
[SwitchD] ntp-service authentication enable
[SwitchD] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[SwitchD] ntp-service reliable authentication-keyid 42
[SwitchD] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

Step 6 Verify the configuration.

After the configurations, Switch B can synchronize its clock with the clock of Switch A.

Check the NTP status of Switch B, and you can view that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch B is 3, one stratum lower than the clock stratum of Switch A.

```
[SwitchB] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 2.2.2.2
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
```

```
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

After the configurations, Switch C can synchronize its clock with the clock of Switch B.

Check the NTP status of Switch C, and you can view that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch C is 4, one stratum lower than the clock stratum of Switch B.

```
[SwitchC] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.0.1
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

Check the NTP status of Switch D, and you can see that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch C is 4, one stratum lower than the clock stratum of Switch B.

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.0.1
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

Check the NTP status of Switch A.

```
[SwitchA] display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 26.50 ms
 peer dispersion: 10.00 ms
 reference time: 12:01:48.377 UTC Mar 2 2006(C7B15D2C.60A15981)
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 2.2.2.2 255.255.255.0
#
```

```
interface  XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service refclock-master 2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#

vlan batch 110 111
#
interface Vlanif110
 ip address 1.0.1.11 255.255.255.0
#
interface Vlanif111
 ip address 10.0.0.1 255.255.255.0
#
interface  XGigabitEthernet0/0/1
 port hybrid pvid vlan 111
 port hybrid untagged vlan 111
#
interface  XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
  network 10.0.0.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 2.2.2.2 authentication-keyid 42
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 111
#
interface Vlanif111
 ip address 10.0.0.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 111
 port hybrid untagged vlan 111
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
vlan batch 111
#
interface Vlanif111
 ip address 10.0.0.3 255.255.255.0
#
interface  XGigabitEthernet0/0/1
 port hybrid pvid vlan 111
 port hybrid untagged vlan 111
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

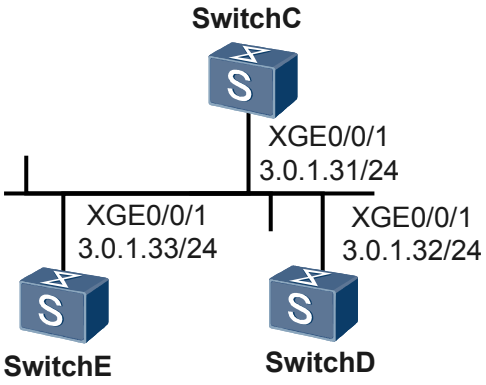
9.4.2 Example for Configuring the Common NTP Peer Mode

Networking Requirements

As shown in **Figure 9-18**, three Switches reside on the LAN.

- The clock of Switch C is the master clock and the clock stratum is 2.
- Switch C is the NTP server of Switch D. That is, Switch D is the client.
- Switch D is the passive peer of Switch E. That is, Switch E is the active end.

Figure 9-18 Networking diagram for configuring the NTP peer mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the clock on Switch C as the master clock. The clock on Switch D should be synchronized to the clock on Switch C.
2. Configure Switch E and Switch D as the NTP peers so that Switch E should send clock synchronization requests to Switch D.

3. The clocks on Switch C, Switch D and Switch E can be synchronized.

Data Preparation

To complete the configuration, you need the following data:

- IP address of Switch C
- IP address of Switch D
- Stratum count of the NTP master clock

Procedure

Step 1 Configure IP addresses for Switch C, Switch D, and Switch E.

Configure an IP address for each interface according to **Figure 9-18**. After configurations, the three Switches can ping each other.

The configuration procedure is not mentioned.

Step 2 Configure the unicast NTP client/server mode.

On Switch C, set the clock as a master NTP clock with stratum being 2.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

Configure Switch C as the NTP server of Switch D.

```
<SwitchD> system-view
[SwitchD] ntp-service unicast-server 3.0.1.31
```

After the configurations, the clock of Switch D is synchronized with the clock of Switch C.

Check the NTP status of Switch D, and you can see that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch D is 3, one stratum lower than the clock stratum of Switch C.

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 3.0.1.31
 nominal frequency: 64.0029 Hz
 actual frequency: 64.0029 Hz
 clock precision: 2^7
 clock offset: 0.0000 ms
 root delay: 62.50 ms
 root dispersion: 0.20 ms
 peer dispersion: 7.81 ms
 reference time: 06:52:33.465 UTC Mar 7 2006(C7B7AC31.773E89A8)
```

Step 3 Configure the unicast NTP peer mode.

Configure Switch D as the passive peer of Switch E.

```
<SwitchE> system-view
[SwitchE] ntp-service unicast-peer 3.0.1.32
```

No master clock is configured on Switch E, so the clock on Switch E should be synchronized to the clock on Switch D.

Step 4 Verify the configuration.

View the status of Switch E after clock synchronization.

Check the NTP status of Switch E, and you can see that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch E is 4, one stratum lower than the clock stratum of Switch D.

```
[SwitchE] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 3.0.1.32
 nominal frequency: 64.0029 Hz
 actual frequency: 64.0029 Hz
 clock precision: 2^7
 clock offset: 0.0000 ms
 root delay: 124.98 ms
 root dispersion: 0.15 ms
 peer dispersion: 10.96 ms
 reference time: 06:55:50.784 UTC Mar 7 2006(C7B7ACF6.C8D002E2)
```

----End

Configuration Files

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 100
#
interface Vlanif100
 ip address 3.0.1.31 255.255.255.0
#
interface  XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100

#
ntp-service refclock-master 2
#
return
```

- Configuration file of Switch D

```
#
 sysname SwitchD
#
vlan batch 100
#
interface Vlanif100
 ip address 3.0.1.32 255.255.255.0
#
interface  XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
 ntp-service unicast-server 3.0.1.31
#
return
```

- Configuration file of Switch E

```
#
 sysname SwitchE
#
vlan batch 100
#
interface Vlanif100
 ip address 3.0.1.33 255.255.255.0
#
interface  XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
```

```
 port hybrid untagged vlan 100
#
 ntp-service unicast-peer 3.0.1.32
#
return
```

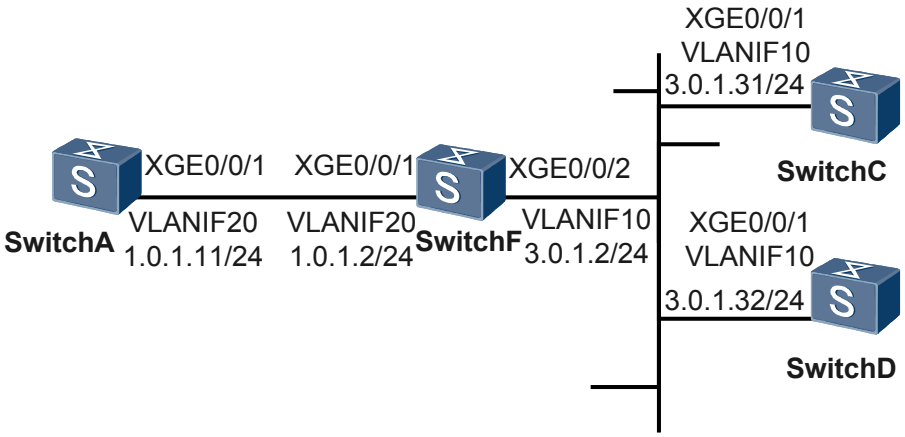
9.4.3 Example for Configuring NTP Authentication in Broadcast Mode

Networking Requirements

As shown in **Figure 9-19**,

- Switch C and Switch D are on the same network segment; Switch A is on another network segment; Switch F connects the two network segments.
- As the NTP broadcast server, Switch C uses the local clock as the NTP master clock, which is a stratum-3 clock. Switch C sends broadcast packets through VLANIF10, namely, XGigabitEthernet0/0/1.
- Switch D uses VLANIF10, namely, XGigabitEthernet0/0/1, to listen to the broadcast packets.
- Switch A uses VLANIF20, namely, XGigabitEthernet0/0/1, to listen to the broadcast packets.
- NTP authentication needs to be enabled.

Figure 9-19 Networking diagram for configuring the NTP broadcast mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch C as the NTP broadcast server.
2. Configure Switch A and Switch D as the NTP broadcast clients.
3. Configure NTP authentication on Switch A, Switch C, and Switch D.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface
- IDs of VLANs to which the interfaces belong
- Stratum count of the NTP master clock
- Authentication key and key ID

Procedure

Step 1 Configure the IP addresses of the Switches.

Configure the IP address of each interface according to **Figure 9-19**.

Configure the IP address of the VLANIF interface on Switch C.

```
<SwitchC> system-view
[SwitchC] vlan 10
[SwitchC-Vlan10] quit
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchC-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchC-XGigabitEthernet0/0/1] quit
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10]ip address 3.0.1.31 24
[SwitchC-Vlanif10]quit
```

Configure the IP address of the VLANIF interface on Switch D.

```
<SwitchD> system-view
[SwitchD] vlan 10
[SwitchD-Vlan10] quit
[SwitchD] interface xgigabitethernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchD-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchD-XGigabitEthernet0/0/1] quit
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] ip address 3.0.1.32 24
[SwitchD-Vlanif10] quit
```

Configure the IP address of the VLANIF interface on Switch F.

```
<SwitchF> system-view
[SwitchF] vlan 10
[SwitchF-Vlan10] quit
[SwitchF] interface xgigabitethernet 0/0/2
[SwitchF-XGigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchF-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchF-XGigabitEthernet0/0/2] quit
[SwitchF] interface vlanif 10
[SwitchF-Vlanif10] ip address 3.0.1.2 24
[SwitchF-Vlanif10] quit
[SwitchF] vlan 20
[SwitchF-Vlan20] quit
[SwitchF] interface xgigabitethernet 0/0/1
[SwitchF-XGigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchF-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchF-XGigabitEthernet0/0/1] quit
[SwitchF] interface vlanif 20
[SwitchF-vlanif20] ip address 1.0.1.2 24
[SwitchF-vlanif20] quit
```

Configure the IP address of the VLANIF interface on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-Vlan20] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 20
[SwitchA-vlanif20] ip address 1.0.1.11 24
[SwitchA-vlanif20] quit
```

Step 2 Configure the routes between them are reachable.The configuration procedure is not mentioned.

Step 3 Configure the NTP broadcast server and enable NTP authentication.

Configure the clock of Switch C as the NTP master clock with the stratum being 3.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 3
```

Enable NTP authentication.

```
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[SwitchC] ntp-service reliable authentication-keyid 16
```

Configure Switch C as an NTP broadcast server. Broadcast packets are encrypted by using the authentication key ID 16 and then sent through VLANIF10.

```
[SwitchC] interface vlanif 10
[SwitchC-vlanif10] ntp-service broadcast-server authentication-keyid 16
[SwitchC-vlanif10] quit
```

Step 4 Configure Switch D, which resides on the same network segment with the server.

Enable NTP authentication.

```
<SwitchD> system-view
[SwitchD] ntp-service authentication enable
[SwitchD] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[SwitchD] ntp-service reliable authentication-keyid 16
```

Configure Switch D as the NTP broadcast client and configure Switch D to listen to NTP broadcast packets through VLANIF10.

```
[SwitchD]interface vlanif 10
[SwitchD-vlanif10] ntp-service broadcast-client
[SwitchD-vlanif10] quit
```

After the configurations, the clock of Switch D is synchronized with the clock of Switch C.

Step 5 Configure Switch A, which resides on different network segment from the server.

Enable NTP authentication.

```
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[SwitchA] ntp-service reliable authentication-keyid 16
```

Configure Switch A as the NTP broadcast client and configure Switch A to listen to NTP broadcast packets through VLANIF20.

```
[SwitchA]interface vlanif 20
[SwitchA-vlanif20] ntp-service broadcast-client
[SwitchA-vlanif20] quit
```

Step 6 Verify the configuration.

After the configurations, the clock on Switch D can be synchronized to the clock on Switch C, but the clock on Switch A cannot be synchronized

because Switch A and Switch C are on different network segments and Switch A cannot receive the broadcast packets sent from Switch C.

Check the NTP status of Switch D, and you can see that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch D is 4, one stratum lower than the clock stratum of Switch C.

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 3.0.1.31
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.42 ms
 peer dispersion: 0.00 ms
 reference time: 12:17:21.773 UTC Mar 7 2006(C7B7F851.C5EAF25B)
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
vlan batch 20
#
interface Vlanif20
 ip address 1.0.1.11 255.255.255.0
 ntp-service broadcast-client
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
#
 ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 16
#
return
```

Configuration file of Switch C

```
#
sysname SwitchC
#
vlan batch 10
#
interface Vlanif10
 ip address 3.0.1.31 255.255.255.0
 ntp-service broadcast-server authentication-keyid 16
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ntp-service authentication enable
```

```
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
ntp-service refclock-master 3
#
return
```

- Configuration file of Switch D

```
#
sysname SwitchD
#
vlan batch 10
#
interface Vlanif10
 ip address 3.0.1.32 255.255.255.0
 ntp-service broadcast-client
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX
\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 16
#
return
```

- Configuration file of Switch F

```
#
sysname SwitchF
#
vlan batch 10 20
#
interface Vlanif10
 ip address 3.0.1.2 255.255.255.0
#
interface Vlanif20
 ip address 1.0.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
  network 3.0.1.0 0.0.0.255
#
return
```

9.4.4 Example for Configuring the Common NTP Multicast Mode

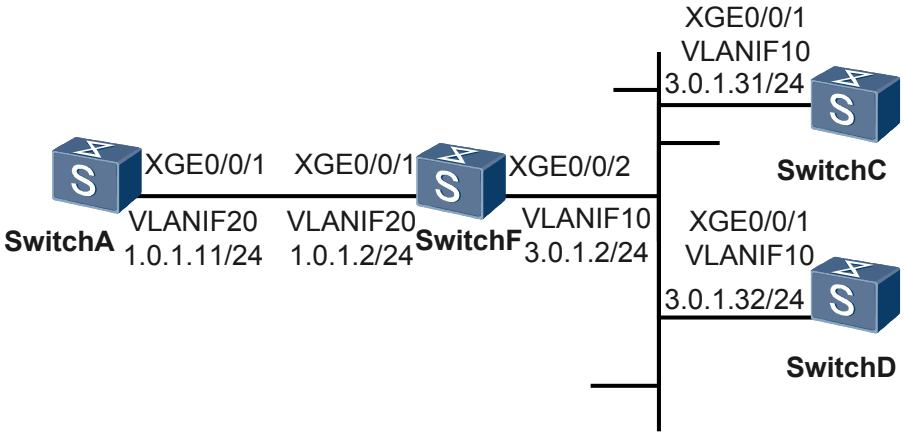
Networking Requirements

As shown in **Figure 9-20**,

- Switch C and Switch D are on the same network segment; Switch A is on another network segment; Switch F connects the two network segments.

- As the NTP multicast server, Switch C uses the local clock as the NTP master clock, which is a stratum-2 clock. Switch C sends multicast packets through VLANIF 10, namely, XGigabitEthernet0/0/1.
- Switch D uses VLANIF 10, namely, XGigabitEthernet0/0/1, to listen to the multicast packets.
- Switch A uses VLANIF 20, namely, XGigabitEthernet0/0/1, to listen to the multicast packets.

Figure 9-20 Networking diagram for configuring the NTP multicast mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch C as the NTP multicast server.
2. Configure Switch A and Switch D as the NTP multicast clients.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface
- Stratum count of the NTP master clock

Procedure

Step 1 Configure the IP addresses of the Switches.

Configure the IP address of each interface according to **Figure 9-20**.

Configure the IP address of the VLANIF interface on Switch C.

```
<SwitchC> system-view
[SwitchC] vlan 10
[SwitchC-Vlan10] quit
[SwitchC] interface xgigabitethernet 0/0/1
[SwitchC-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchC-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchC-XGigabitEthernet0/0/1] quit
```

```
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10]ip address 3.0.1.31 24
[SwitchC-Vlanif10]quit
```

Configure the IP address of the VLANIF interface on Switch D.

```
<SwitchD> system-view
[SwitchD] vlan 10
[SwitchD-Vlan10] quit
[SwitchD] interface xgigabitethernet 0/0/1
[SwitchD-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchD-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchD-XGigabitEthernet0/0/1] quit
[SwitchD] interface vlanif 10
[SwitchD-Vlanif10] ip address 3.0.1.32 24
[SwitchD-Vlanif10] quit
```

Configure the IP address of the VLANIF interface on Switch F.

```
<SwitchF> system-view
[SwitchF] vlan 10
[SwitchF-Vlan10] quit
[SwitchF] interface xgigabitethernet 0/0/2
[SwitchF-XGigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchF-XGigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchF-XGigabitEthernet0/0/2] quit
[SwitchF] interface vlanif 10
[SwitchF-Vlanif10] ip address 3.0.1.2 24
[SwitchF-Vlanif10] quit
[SwitchF] vlan 20
[SwitchF-Vlan20] quit
[SwitchF] interface xgigabitethernet 0/0/1
[SwitchF-XGigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchF-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchF-XGigabitEthernet0/0/1] quit
[SwitchF] interface vlanif 20
[SwitchF-vlanif20] ip address 1.0.1.2 24
[SwitchF-vlanif20] quit
```

Configure the IP address of the VLANIF interface on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-Vlan20] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 20
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 20
[SwitchA-XGigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 20
[SwitchA-vlanif20] ip address 1.0.1.11 24
[SwitchA-vlanif20] quit
```

Step 2 Configure the routes between them are reachable.The configuration procedure is not mentioned.

Step 3 Configure the NTP multicast server.

Configure the clock of Switch C as the NTP master clock with the stratum being 2.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

Configure Switch C as the NTP multicast client and configure Switch C to sense NTP multicast packets through VLANIF10.

```
[SwitchC] interface vlanif 10
[SwitchC-vlanif10] ntp-service multicast-server
[SwitchC-vlanif10] quit
```

Step 4 Configure Switch D, which resides on the same network segment with the server.

Configure Switch D as the NTP multicast client and configure Switch D to sense NTP multicast packets through VLANIF10.

```
<SwitchD> system-view
[SwitchD] interface vlanif 10
[SwitchD-vlanif10] ntp-service multicast-client
[SwitchD-vlanif10] quit
```

Step 5 Configure Switch A, which resides on different network segment from the server.

Configure Switch A as the NTP multicast client and configure Switch A to sense NTP multicast packets through VLANIF20.

```
<SwitchA> system-view
[SwitchA] interface vlanif 20
[SwitchA-vlanif20] ntp-service multicast-client
[SwitchA-vlanif20] quit
```

Step 6 Verify the configuration.

After the configurations, the clock on Switch D can be synchronized to the clock on Switch C, but the clock on Switch A cannot be synchronized

because Switch A and Switch C are on different network segments and Switch A cannot receive the multicast packets sent from Switch C.

Check the NTP status of Switch D, and you can see that the status of the clock is synchronized. This means that the synchronization is complete. The stratum of the clock of Switch D is 3, one stratum lower than the clock stratum of Switch C.

```
[SwitchD] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 3.0.1.31
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.66 ms
 root delay: 24.47 ms
 root dispersion: 208.39 ms
 peer dispersion: 9.63 ms
 reference time: 17:03:32.022 UTC Apr 25 2005(C61734FD.800303C0)
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
vlan batch 20
#
interface Vlanif20
 ip address 1.0.1.11 255.255.255.0
 ntp-service multicast-client
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
sysname SwitchC
#
vlan batch 10
#
 ntp-service refclock-master  2
#
interface Vlanif10
 ip address 3.0.1.31 255.255.255.0
 ntp-service multicast-server
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- Configuration file of Switch D

```
#
sysname SwitchD
#
vlan batch 10
#
interface Vlanif10
 ip address 3.0.1.32 255.255.255.0
 ntp-service multicast-client
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
Return
```

Configuration file of Switch F

```
#
sysname SwitchF
#
vlan batch 10 20
#
interface Vlanif10
 ip address 3.0.1.2 255.255.255.0
#
interface Vlanif20
 ip address 1.0.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ospf 1
 area 0.0.0.0
  network 1.0.1.0 0.0.0.255
  network 3.0.1.0 0.0.0.255
#
return
```

9.5 Ping and Tracert

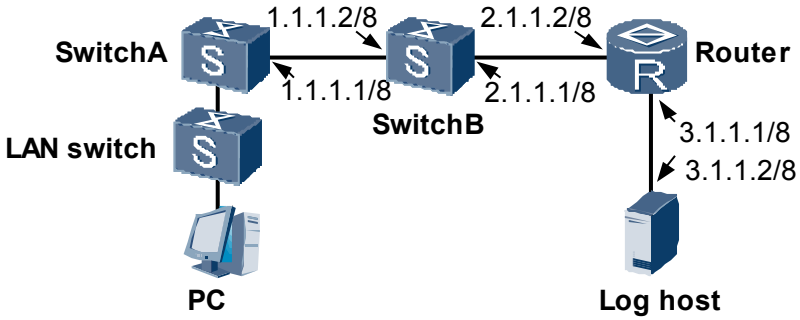
This chapter describes basic concepts and applications of the **ping** and **tracert** commands.

9.5.1 Example for Performing Ping and Tracert Operations

Networking Requirements

As shown in **Figure 9-21**, after configuring Switch A, you check the link between Switch A and the log host. If Switch A and the log host are disconnected, you cannot know which device fails because there are other network devices between Switch A and the log host. To locate on which link segment the fault occurs, you can perform ping and tracert operations.

Figure 9-21 Networking diagram of ping and tracert operations



Configuration Roadmap

The configuration roadmap is as follows:

1. Run the **ping** command on Switch A to check the connectivity between Switch A and the log host.
2. Run the **tracert** command to locate the fault after you find that the link is faulty.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the interfaces on Switch B (In this example, IP addresses of the interfaces are 1.1.1.2/8 and 2.1.1.1/8.)
- IP addresses of the interfaces on Router (In this example, IP addresses of the interfaces are 2.1.1.2/8 and 3.1.1.1/8.)
- IP address of the log host (In this example, the IP address of the log host is 3.1.1.2/8.)

Procedure

Step 1 Run the **ping** command.

Run the **ping** command on Switch A to check the connectivity between Switch A and the log host.

```
<Quidway> ping 3.1.1.2
  PING 3.1.1.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
```

```
  Request time out
  Request time out

--- 3.1.1.2 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

The display on Switch A shows that the log host is unreachable, which indicates that a fault occurs on some link segment between Switch A and the log host.

Step 2 Run the **tracert** command.

Run the **tracert** command on Switch A to locate which link segment fails.

```
<Quidway> tracert 3.1.1.2
 traceroute to 3.1.1.2(3.1.1.2), max hops: 30 ,packet length: 40
 1 1.1.1.2             4 ms  5 ms  5 ms
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
...
```

The preceding display shows that the ICMP Echo Request message passes Switch B but does not reach Router. It indicates that the link between Switch B and Router fails. After the link between Switch B and Router is recovered, you can repeat Step 1 and Step 2 to ensure that Switch A and the log host can communicate properly.

----End

Configuration Files

None.

9.6 NQA Configuration

This chapter describes how to configure the Network Quality Analysis (NQA) to monitor the network operating status and collect network operation indexes in real time.

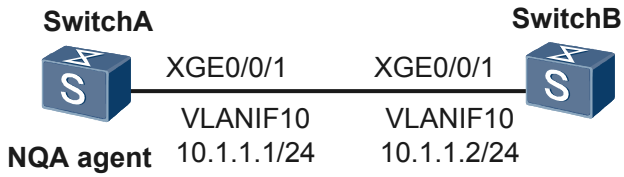
9.6.1 Example for Configuring the ICMP Test

Networking Requirements

As shown in **Figure 9-22**, Switch A and Switch B must be connected at Layer 3 through the VLANIF interface.

Switch A functions as the NQA client to check whether Switch B is reachable.

Figure 9-22 Networking diagram for configuring the ICMP test



Configuration Roadmap

The configuration roadmap is as follows:

1. Perform the NQA ICMP test to check whether the route between the local end (Switch A) and the specified destination end (Switch B) is reachable and check the RTT of a test packet.

Data Preparation

To complete the configuration, you need the following data:

- Host address of Switch B

Procedure

Step 1 Create a VLAN and add interfaces to the VLAN.

Configure Switch A.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-Vlan10] quit
[SwitchA] interface xgigabitethernet 0/0/1
[SwitchA-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-XGigabitEthernet0/0/1] quit
```

Configure Switch B.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 10
[SwitchB-Vlan10] quit
[SwitchB] interface xgigabitethernet 0/0/1
[SwitchB-XGigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchB-XGigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchB-XGigabitEthernet0/0/1] quit
```

Step 2 Configure the VLANIF interface and assign an IP address to the VLANIF interface.

Configure Switch A.

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 24
```

Configure Switch B.

```
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 10.1.1.2 24
```

Step 3 Enable the NQA client and create an NQA ICMP test.

```
[SwitchA] nqa test-instance admin icmp
[SwitchA-nqa-admin-icmp] test-type icmp
[SwitchA-nqa-admin-icmp] destination-address ipv4 10.1.1.2
```

Step 4 Perform the test immediately.

```
[SwitchA-nqa-admin-icmp] start now
```

Step 5 Verify the test result.

```
[SwitchA-nqa-admin-icmp] display nqa results test-instance admin icmp
```

```
NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
 1 . Test 1 result   The test is finished
  Send operation times: 3              Receive response times: 3
  Completion:success                   RTD OverThresholds number: 0
  Attempts number:1                    Drop operation number:0
  Disconnect operation number:0        Operation timeout number:0
  System busy operation number:0       Connection fail number:0
  Operation sequence errors number:0   RTT Stats errors number:0
  Destination ip address:10.1.1.2
  Min/Max/Average Completion Time: 1/30/17
  Sum/Square-Sum  Completion Time: 51/1301
  Last Good Probe Time: 2010-06-09 19:27:48.1
  Lost packet ratio: 0 %
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
sysname SwitchB
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

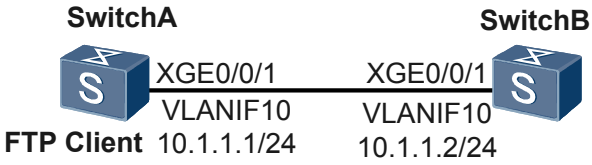
9.6.2 Example for Configuring the FTP Download Test

Networking Requirements

As shown in **Figure 9-23**:

- Switch B functions as the FTP server.
- A user with the name **user1** and the password **hello** intends to log in to the FTP server to download the **test.txt** file.

Figure 9-23 Networking diagram for configuring the FTP download test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch A as the NQA client.
2. Create and perform the FTP test on Switch A to check whether a connection between Switch A and the FTP server can be set up and to check the time for downloading a file from the FTP server.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the FTP server
- Source IP address for the test
- FTP user name and password
- Operation file of the FTP test

Procedure

Step 1 Configure the IP addresses of Switch A and Switch B. The configuration details are not mentioned here.

Step 2 Configure Switch B as the FTP server.

```
<SwitchB> system-view
[SwitchB] ftp server enable
[SwitchB] aaa
[SwitchB-aaa] local-user user1 password cipher hello
[SwitchB-aaa] local-user user1 service-type ftp
[SwitchB-aaa] local-user user1 ftp-directory flash:
[SwitchB-aaa] quit
```

Step 3 Configure an NQA FTP test on Switch A.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin ftp
[SwitchA-nqa-admin-ftp] test-type ftp
[SwitchA-nqa-admin-ftp] destination-address ipv4 10.1.1.2
[SwitchA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[SwitchA-nqa-admin-ftp] ftp-operation get
[SwitchA-nqa-admin-ftp] ftp-username user1
[SwitchA-nqa-admin-ftp] ftp-password hello
[SwitchA-nqa-admin-ftp] ftp-filename test.txt
```

Step 4 Perform the test.

```
[SwitchA-nqa-admin-ftp] start now
```

Step 5 Verify the test result.

```
[SwitchA-nqa-admin-ftp] display nqa results test-instance admin ftp
 NQA entry(admin, ftp) :testflag is inactive ,testtype is  ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                           ResponseProbe:1
   Completion :success                   RTD OverThresholds number: 0
   MessageBodyOctetsSum: 448             Stats errors number: 0
   Operation timeout number: 0           System busy operation number:0
   Drop operation number:0               Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 438/438/438
   DataConnTime Min/Max/Average: 218/218/218
   SumTime Min/Max/Average: 656/656/656
   Average RTT:656
   Lost packet ratio:0 %
```

----End

Configuration Files

- Configuration file of Switch A

```
#
sysname SwitchA
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin ftp
 test-type  ftp
 destination-address ipv4 10.1.1.2
 source-address ipv4 10.1.1.1
 ftp-username user1
 ftp-password hello
 ftp-filename test.txt
 ftp-operation get
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
 FTP server enable
#
aaa
 local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 local-user user1 service-type ftp
 local-user user1 ftp-directory flash:
 #
return
```

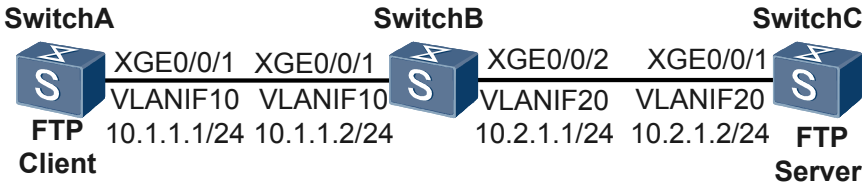
9.6.3 Example for Configuring the FTP Upload Test

Networking Requirements

As shown in **Figure 9-24**:

You are required to test the speed of uploading a file from Switch C to the FTP server.

Figure 9-24 Networking diagram for configuring the FTP upload test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch A as the NQA client and the FTP client. Create and perform the FTP test on Switch A to check whether a connection between Switch A and the FTP server can be set up and to test the time for uploading a file to the FTP server.
2. A user with the name **user1** and the password **hello** logs in to the FTP server to upload a file whose size is 10k.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the FTP server
- Source IP address for the test
- FTP user name and password
- Size of the uploaded file

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Configure Switch C as the FTP server.

```
<SwitchC> system-view
[SwitchC] ftp server enable
[SwitchC] aaa
[SwitchC-aaa] local-user user1 password cipher hello
[SwitchC-aaa] local-user user1 service-type ftp
[SwitchC-aaa] local-user user1 ftp-directory flash:
[SwitchC-aaa] quit
```

Step 3 Configure an NQA FTP test on Switch A and create a file of 10K bytes for uploading.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin ftp
```

```
[SwitchA-nqa-admin-ftp] test-type ftp
[SwitchA-nqa-admin-ftp] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[SwitchA-nqa-admin-ftp] ftp-operation put
[SwitchA-nqa-admin-ftp] ftp-username user1
[SwitchA-nqa-admin-ftp] ftp-password hello
[SwitchA-nqa-admin-ftp] ftp-filename nqa-ftp-test.txt
[SwitchA-nqa-admin-ftp] ftp-filesize 10
```

Step 4 Perform the test.

```
[SwitchA-nqa-admin-ftp] start now
```

Step 5 Verify the test result.

Verify the NQA test result on Switch A.

```
[SwitchA-nqa-admin-ftp] display nqa results test-instance admin ftp
 NQA entry(admin, ftp) :testflag is inactive ,testtype is  ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                          ResponseProb:1
   Completion :success                  RTD OverThresholds number: 0
   MessageBodyOctetsSum: 10240          Stats errors number: 0
   Operation timeout number: 0          System busy operation number:0
   Drop operation number:0              Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 657/657/657
   DataConnTime Min/Max/Average: 500/500/500
   SumTime Min/Max/Average: 1157/1157/1157
   Average RTT:1157
   Lost packet ratio:0 %
```

On Switch C, you can see that a file named **nqa-ftp-test.txt** is added.

```
<SwitchC> dir
Directory of flash:

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
   0   -rw-            331  Feb 06 2009 18:34:34   private-data.txt
   1   -rw-          10240  Feb 06 2009 18:37:06   nqa-ftp-test.txt

2540 KB total (1536 KB free)
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin ftp
 test-type  ftp
 destination-address ipv4 10.2.1.2
 source-address ipv4 10.1.1.1
 ftp-filesize 10
 ftp-username user1
 ftp-password hello
 ftp-filename nqa-ftp-test.txt
 ftp-operation put
#
```

```
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

- Configuration file of Switch C

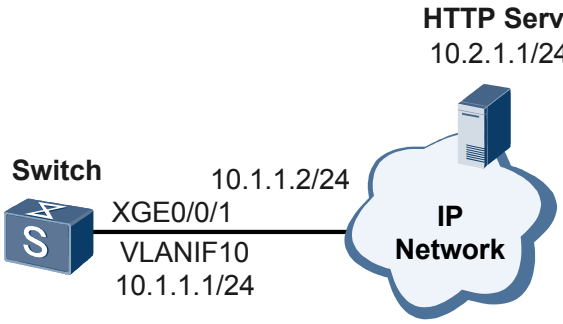
```
#
 sysname SwitchC
#
 FTP server enable
#
 vlan batch 20
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
aaa
 local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 local-user user1 service-type ftp
 local-user user1 ftp-directory flash:
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

9.6.4 Example for Configuring the HTTP Test

Networking Requirements

As shown in **Figure 9-25**, Switch is connected to the HTTP server through a WAN.

Figure 9-25 Networking diagram for configuring the HTTP test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Switch as the NQA client.
2. Create and perform the HTTP test on the Switch to check whether the a connection between the Switch and the HTTP server can be set up and to check the time for transferring a file between them.

Data Preparation

To complete the configuration, you need the following data:

- Host address of the HTTP server
- HTTP operation type

Procedure

Step 1 Configure reachable routes between Switch and HTTP Server. The configuration details are not mentioned here.

Step 2 Enable the NQA client and create an NQA HTTP test.

```
<Quidway> system-view
[Quidway] nqa test-instance admin http
[Quidway-nqa-admin-http] test-type http
[Quidway-nqa-admin-http] destination-address ipv4 10.2.1.1
[Quidway-nqa-admin-http] http-operation get
[Quidway-nqa-admin-http] http-url www.huawei.com
```

Step 3 Perform the test.

```
[Quidway-nqa-admin-http] start now
```

Step 4 Verify the test result.

```
[Quidway-nqa-admin-http] display nqa results test-instance admin http
 NQA entry(admin, http) :testflag is inactive ,testtype is http
  1 . Test 1 result   The test is finished
   SendProbe:3                          ResponseProbe:3
   Completions: success                 RTD OverThresholdsnumber: 0
   MessageBodyOctetsSum: 0              TargetAddress: 10.2.1.1
   DNSQueryError number: 0              HTTPError number: 0
   TcpConnError number : 3              System busy operation number:0
   DNSRTT Sum/Min/Max:0/0/0             TCPConnectRTT Sum/Min/Max: 0/0/0
   TransactionRTT Sum/Min/Max: 11/3/4
```

```
  RTT Sum/Min/Max/Avg: 18/5/7/6
  DNSServerTimeout:0  TCPConnectTimeout:0  TransactionTimeout: 0
  Lost packet ratio:0%
```

----End

Configuration Files

Configuration file of Switch

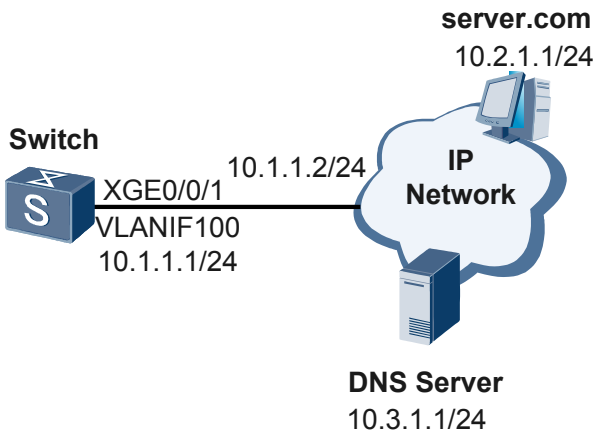
```
#
sysname quidway
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
nqa test-instance admin http
 test-type http
 destination-address ipv4 10.2.1.1
 http-operation get
 http-url www.huawei.com
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

9.6.5 Example for Configuring the DNS Test

Networking Requirements

As shown in **Figure 9-26**, Switch functions as the DNS client to access the host whose IP address is 10.2.1.1/24 through a domain named **server.com**.

Figure 9-26 Networking diagram for configuring the DNS test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Switch as the NQA client.
2. Create and perform the DNS test on the Switch to check whether a connection between the Switch and the DNS server can be set up and to check the speed of responding to an address resolution request.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the DNS server
- Name of the host to be accessed

Procedure

Step 1 Configure reachable routes between Switch A and the DNS server, between Switch A and the host to be accessed, and between the DNS server and the host to be accessed. The configuration details are not mentioned here.

Step 2 Create an NQA DNS test.

```
<Quidway> system-view
[Quidway] dns server 10.3.1.1
[Quidway] nqa test-instance admin dns
[Quidway-nqa-admin-dns] test-type dns
[Quidway-nqa-admin-dns] dns-server ipv4 10.3.1.1
[Quidway-nqa-admin-dns] destination-address url server.com
```

Step 3 Perform the test.

```
[Quidway-nqa-admin-dns] start now
```

Step 4 Verify the test result.

```
[Quidway] display nqa results test-instance admin dns

 NQA entry(admin, dns) :testflag is inactive ,testtype is dns
  1 . Test 1 result   The test is finished
   Send operation times: 1              Receive response times: 1
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:
10.3.1.1
   Min/Max/Average Completion Time: 1/1/1
   Sum/Square-Sum  Completion Time: 1/1
   Last Good Probe Time: 2009-2-3 10:52:5.7
   Lost packet ratio: 0 %
```

----End

Configuration Files

Configuration file of Switch

```
#
 sysname Quidway
#
 dns server 10.3.1.1
```

```
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin dns
 test-type dns
 destination-address url server.com
 dns-server ipv4 10.3.1.1
#
 ip route-static 10.3.1.0 255.255.255.0 10.1.1.2
#
return
```

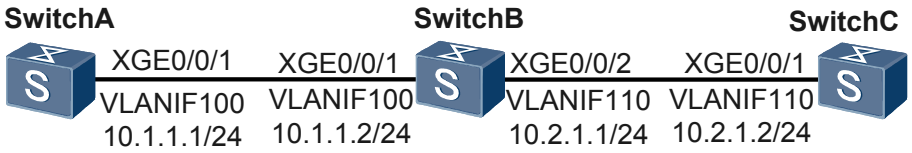
9.6.6 Example for Configuring the Traceroute Test

Networking Requirements

As shown in **Figure 9-27**:

The traceroute test is used to check the IP address of the VLANIF 110 interface of Switch C on Switch A.

Figure 9-27 Networking diagram for configuring the traceroute test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch A as the NQA client.
2. Create and perform the traceroute test on Switch A to check the statistics on each hop from Switch A to Switch C.

Data Preparation

To complete the configuration, you need the following data:

- Destination address for the traceroute test

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Create an NQA traceroute test on Switch A and set the destination IP address to **10.2.1.2**.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin trace
[SwitchA-nqa-admin-trace] test-type trace
[SwitchA-nqa-admin-trace] destination-address ipv4 10.2.1.2
```

Step 3 Perform the test.

```
[SwitchA-nqa-admin-trace] start now
```

Step 4 Verify the test result.

Verify the NQA test result on Switch A.

```
[SwitchA-nqa-admin-trace] display nqa results test-instance admin trace
 NQA entry(admin, trace) :testflag is inactive ,testtype is trace
  1 . Test 1 result   The test is finished
   Completion:success                    Attempts number:1
   Disconnect operation number:0         Operation timeout number:0
   System busy operation number:0        Connection fail number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   Drop operation number:0
   Last good path Time:2006-8-5 14:38:58.5
   1 . Hop 1
    Send operation times: 3              Receive response times: 3
    Min/Max/Average Completion Time: 46/47/41
    Sum/Square-Sum  Completion Time: 125/5349
    RTD OverThresholds number: 0
    Last Good Probe Time: 2006-8-5 14:38:58.3
    Destination ip address:10.1.1.2
    Lost packet ratio: 0 %
   2 . Hop 2
    Send operation times: 3              Receive response times: 3
    Min/Max/Average Completion Time: 31/79/62
    Sum/Square-Sum  Completion Time: 188/13286
    RTD OverThresholds number: 0
    Last Good Probe Time: 2006-8-5 14:38:58.5
    Destination ip address:10.2.1.2
    Lost packet ratio: 0 %
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin trace
 test-type  trace
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 100 110
```

```
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- Configuration file of Switch C

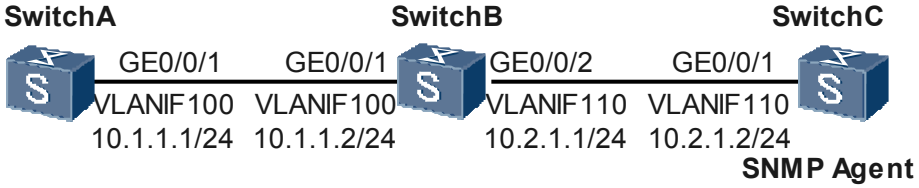
```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

9.6.7 Example for Configuring the SNMP Query Test

Networking Requirements

As shown in **Figure 9-28**, SNMP agent is enabled on Switch C. The NQA SNMP query test is used to measure the time from sending an SNMP query packet to receiving an Echo packet.

Figure 9-28 Networking diagram for configuring the SNMP query test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch A as the NQA client.
2. Create and perform the SNMP query test on Switch A.
3. Enable SNMP agent on Switch C.

Data Preparation

To complete the configuration, you need the following data:

- Host address of the SNMP agent

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Enable SNMP agent on Switch C.

```
<SwitchC> system-view
[SwitchC] snmp-agent
```

Step 3 Create an SNMP query test on Switch A.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin snmp
[SwitchA-nqa-admin-snmp] test-type snmp
[SwitchA-nqa-admin-snmp] destination-address ipv4 10.2.1.2
```

Step 4 Perform the test.

```
[SwitchA-nqa-admin-snmp] start now
```

Step 5 Verify the test result.

```
[SwitchA-nqa-admin-snmp] display nqa results test-instance admin snmp
 NQA entry(admin, snmp) :testflag is inactive ,testtype is snmp
  1 . Test 1 result   The test is finished
   Send operation times: 3                Receive response times: 3
   Completion:success                      RTD OverThresholds number: 0
   Attempts number:1                       Drop operation number:0
   Disconnect operation number:0         Operation timeout number:0
   System busy operation number:0        Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 63/172/109
   Sum/Square-Sum  Completion Time: 329/42389
   Last Good Probe Time: 2006-8-5 15:33:49.1
   Lost packet ratio: 0 %
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin snmp
 test-type snmp
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
```

```
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- Configuration file of Switch C

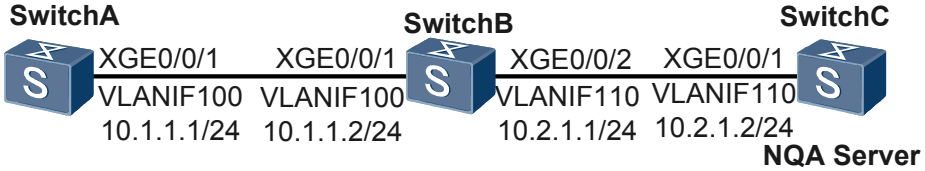
```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100006294
 snmp-agent sys-info version v3
#
return
```

9.6.8 Example for Configuring the TCP Test

Networking Requirements

As shown in **Figure 9-29**, the NQA TCP Private test is used to obtain the time for setting up a TCP connection between Switch A and Switch B.

Figure 9-29 Networking diagram for configuring the TCP test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch A as the NQA client and configure Switch C as the NQA server.
2. Configure the monitoring port number on the NQA server and create an NQA TCP test on the NQA client.

Data Preparation

To complete the configuration, you need the following data:

- Host address of the server
- Port number used to monitor the TCP service on the server

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Configure the NQA server on Switch C.

Configure the IP address and port number used to monitor TCP connections on the NQA server.

```
<SwitchC> system-view
[SwitchC] nqa-server tcpconnect 10.2.1.2 9000
```

Step 3 # Configure Switch A.

Enable the NQA client and create a TCP Private test.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin tcp
[SwitchA-nqa-admin-tcp] test-type tcp
[SwitchA-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-tcp] destination-port 9000
```

Step 4 Perform the test.

```
[SwitchA-nqa-admin-tcp] start now
```

Step 5 Verify the test result.

```
[SwitchA-nqa-admin-tcp] display nqa results test-instance admin tcp
 NQA entry(admin, tcp) :testFlag is inactive ,testtype is tcp
  1 . Test 1 result   The test is finished
   Send operation times: 3               Receive response times: 3
   Completion:success                    RTD OverThresholds number: 0
   Attempts number:1                     Drop operation number:0
   Disconnect operation number:0         Operation timeout number:0
   System busy operation number:0        Connection fail number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 46/63/52
   Sum/Square-Sum  Completion Time: 156/8294
   Last Good Probe Time: 2006-8-5 15:53:17.8
   Lost packet ratio: 0 %
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin tcp
 test-type tcp
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- Configuration file of Switch C

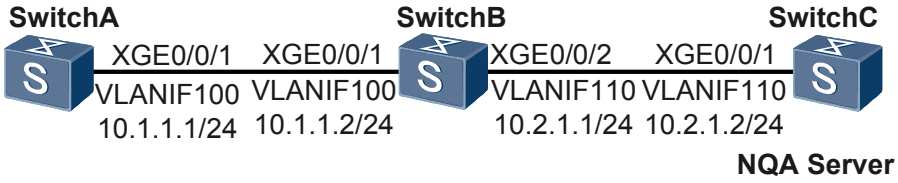
```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 nqa-server tcpconnect 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

9.6.9 Example for Configuring the UDP Test

Networking Requirements

As shown in **Figure 9-30**, the NQA UDP Public test is used to obtain RTT of a UDP packet transmitted between Switch A and Switch C.

Figure 9-30 Networking diagram for configuring the UDP test



Configuration Roadmap

1. Configure Switch A as the NQA client and configure Switch C as the NQA server.
2. Configure the monitoring port number on the NQA server and create an NQA UDP Public test on the NQA client.

Data Preparation

To complete the configuration, you need the following data:

- Host address of the server
- Port number used to monitor the UDP service on the server

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Configure the NQA server on Switch C.

Configure the IP address and UDP port number monitored by the NQA server.

```
<SwitchC> system-view
[SwitchC] nqa-server udpecho 10.2.1.2 6000
```

Step 3 # Configure Switch A.

Enable the NQA client and create a UDP Public test.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin udp
[SwitchA-nqa-admin-udp] test-type udp
[SwitchA-nqa-admin-udp] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-udp] destination-port 6000
```

Step 4 Perform the test.

```
[SwitchA-nqa-admin-udp] start now
```

Step 5 Verify the test result.

```
[SwitchA-nqa-admin-udp] display nqa results test-instance admin udp
 NQA entry(admin, udp) :testflag is inactive ,testtype is udp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
```

```
Min/Max/Average Completion Time: 32/109/67
Sum/Square-Sum  Completion Time: 203/16749
Last Good Probe Time: 2006-8-5 16:9:21.6
Lost packet ratio: 0 %
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.2.1.2
 destination-port 6000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
 nqa-server udpecho 10.2.1.2 6000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
```

```
#
return
```

9.6.10 Example for Configuring the Jitter Test

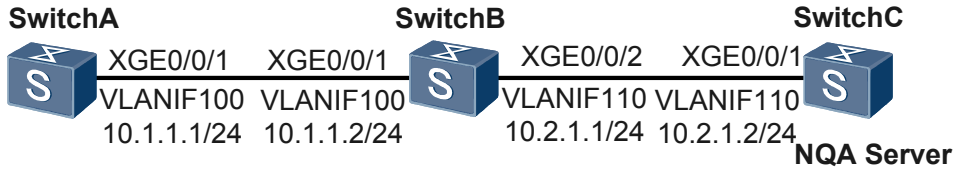
Networking Requirements

As shown in **Figure 9-31**, the NQA Jitter test needs to be used to obtain the jitter time of transmitting a packet from Switch A to Switch C. Switch A and Switch C synchronize the clock from Switch B so that the test precision is improved.

NOTE

For information about clock synchronization, see "NTP" in the *Quidway S6700 Series Ethernet Switches Feature Description - Network Management*.

Figure 9-31 Networking diagram for configuring the Jitter test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch C as the NTP client and configure Switch B as the NTP server.
2. Configure Switch A as the NQA client and configure Switch C as the NQA server.
3. Configure the service type and port number monitored by the NQA server.
4. Create and perform the NQA Jitter test on the NQA client.

Data Preparation

To complete the configuration, you need the following data:

- Host address of the server
- Port number used to monitor the UDP service on the server

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Configure the NQA server on Switch C.

Configure the IP address and UDP port number monitored by the NQA server.

```
<SwitchC> system-view
[SwitchC] nqa-server udpecho 10.2.1.2 9000
```

Step 3 # Configure Switch A.

Enable the NQA client and create an NQA Jitter test.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin jitter
[SwitchA-nqa-admin-jitter] test-type jitter
[SwitchA-nqa-admin-jitter] destination-address ipv4 10.2.1.2
[SwitchA-nqa-admin-jitter] destination-port 9000
```

Step 4 Perform the test.

```
[SwitchA-nqa-admin-jitter] start now
```

Step 5 Verify the test result.

```
[SwitchA-nqa-admin-jitter] display nqa results test-instance admin jitter

 NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion:success                    RTD OverThresholds number:0
   Min/Max/Avg/Sum RTT:1/98/8/461        RTT  Square Sum:23037
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:96                    Max Positive DS:8
   Positive SD Number:15                 Positive DS Number:8
   Positive SD Sum:172                   Positive DS Sum:18
   Positive SD Square Sum :9868          Positive DS Square Sum :86
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:20                    Max Negative DS:10
   Negative SD Number:18                 Negative DS Number:8
   Negative SD Sum:163                   Negative DS Sum:28
   Negative SD Square Sum :2519          Negative DS Square Sum :194
   Min Delay SD:0                        Min Delay DS:0
   Avg Delay SD:3                        Avg Delay DS:3
   Max Delay SD:49                       Max Delay DS:48
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 jitter out value:5.1291060
   jitter in value:0.6602845             NumberOfOWD:60
   OWD SD Sum:206                        OWD DS Sum:195
   TimeStamp unit: ms
```

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
 vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
 vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
return
```

- Configuration file of Switch C

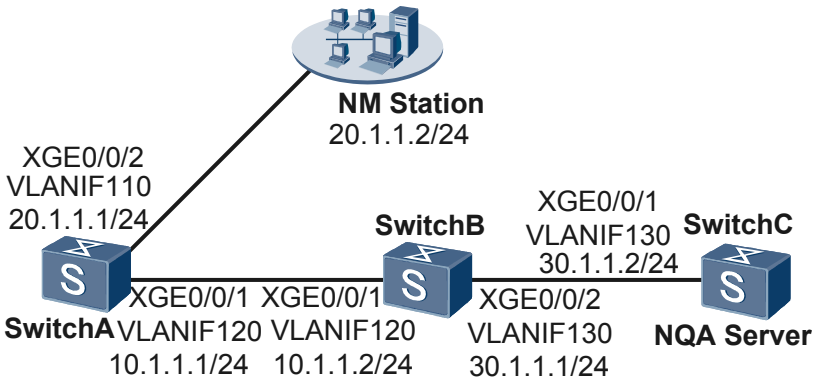
```
#
 sysname SwitchC
#
 vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
  nqa-server udpecho 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

9.6.11 Example for Configuring the Test of Sending NQA Threshold Traps to the NMS

Networking Requirements

As shown in **Figure 9-32**, the trap threshold are configured and the function of sending trap messages is enabled when a Jitter test is configured. After the Jitter test is complete, Switch A sends a trap message to the NMS when the interval for transmitting the test packet from Switch A to Switch C or from Switch C to Switch A exceeds the configured unidirectional transmission threshold, or when the RTT of the test packet exceeds the configured bidirectional transmission threshold. Network administrators can view the cause of a trap in the trap message received by the NMS.

Figure 9-32 Network diagram for configuring the NQA threshold



NOTE

For the information about clock synchronization, see "NTP" in the *Quidway S6700 Series Ethernet Switches Feature Description - Network Management*.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a Jitter test.
2. Configure the NQA thresholds.
3. Enable the function of sending trap messages.
4. Configure the function of sending trap messages to the NMS.

Data Preparation

To complete the configuration, you need the following data:

- IP address and port number of the server-side host.
- Type of the monitored service and monitoring port number
- RTD threshold and OWD threshold
- IP address of the NMS

Procedure

Step 1 Configure reachable routes between Switch A and Switch B, between Switch A and Switch C, and between Switch B and Switch C. The configuration details are not mentioned here.

Step 2 Configure a Jitter test.

Configure the IP address and UDP port number monitored by the NQA server on Switch C.

```
<SwitchC> system-view
[SwitchC] nqa-server udpecho 30.1.1.2 9000
```

Enable the NQA client on Switch A and create an NQA Jitter test on it.

```
<SwitchA> system-view
[SwitchA] nqa test-instance admin jitter
[SwitchA-nqa-admin-jitter] test-type jitter
```

```
[SwitchA-nqa-admin-jitter] destination-address ipv4 30.1.1.2
[SwitchA-nqa-admin-jitter] destination-port 9000
```

Step 3 Configure the NQA thresholds.

Configure the RTD threshold on Switch A.

```
[SwitchA-nqa-admin-jitter] threshold rtd 20
```

Step 4 Enable the function of sending trap messages.

```
[SwitchA-nqa-admin-jitter] send-trap rtd
[SwitchA-nqa-admin-jitter] quit
```

Step 5 Configure the function of sending trap messages to the NMS.

```
[SwitchA] snmp-agent trap enable
[SwitchA] snmp-agent sys-info version v2c
[SwitchA] snmp-agent target-host trap address udp-domain 20.1.1.2 params
securityname public v2c
```

Step 6 Perform the test.

```
[SwitchA] nqa test-instance admin jitter
[SwitchA-nqa-admin-jitter] start now
[SwitchA-nqa-admin-jitter] quit
[SwitchA] quit
```

Step 7 Verify the configuration.

Verify the NQA test result of each Switch.

```
<SwitchA> display nqa results

NQA entry(test, jitter) :testflag is inactive ,testtype is jitter
 1 . Test 1 result   The test is finished
   Send operation times:3000            Receive response times:3000
   Completion :success                  RTD RTD OverThresholds number:25
   Min/Max/Avg/Sum RTT:1/26/1/3143      RTT  Square Sum:5665
   NumOfRTT:3000                        Drop operation number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   System busy operation number:0       Operation timeout number:0
   Min Positive SD:1                    Min Positive DS:0
   Max Positive SD:27                   Max Positive DS:0
   Positive SD Number:1890              Positive DS Number:0
   Positive SD Sum:2128                 Positive DS Sum:0
   Positive SD Square Sum :4864         Positive DS Square Sum :0
   Min Negative SD:1                    Min Negative DS:1
   Max Negative SD:16                   Max Negative DS:2
   Negative SD Number:38                Negative DS Number:1936
   Negative SD Sum:129                  Negative DS Sum:1998
   Negative SD Square Sum :1445         Negative DS Square Sum :2122
   Min Delay SD:0                       Min Delay DS:0
   Avg Delay SD:0                       Avg Delay DS:0
   Max Delay SD:13                      Max Delay DS:12
   Packet Loss SD:0                     Packet Loss DS:0
   Packet Loss Unknown:0                Average of Jitter:1
   Packet Loss Unknown:0                jitter out value:0.7489559
   jitter in value:0.6627117            NumberOfOWD:0
   OWD SD Sum:81                        OWD DS Sum:62
   TimeStamp unit: ms
```

Verify that a trap message is generated in the trap buffer.

```
<Quidway> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
```

```
Current messages : 3

#Jul  9 00:28:34 2009 Quidway  NQA/4/RTDTHRESHOLD:OID
1.3.6.1.4.1.2011.5.25.111.6.16 NQA entry RTD over threshold. (OwnerIndex=admin,
TestName=jitter)
#Jul  9 00:28:34 2009 Quidway NQA/4/SDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.17
NQA entry OWD-SD over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Quidway  NQA/4/DSTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.
18 NQA entry OWD-DS over threshold. (OwnerIndex=admin, TestName=jitter)
```

Verify that the NMS can receive the trap message successfully. The displayed information is not provided here.

----End

Configuration Files

- Configuration file of Switch A

```
#
 sysname SwitchA
#
vlan batch 110 120
#
interface Vlanif110
 ip address 20.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.1.1 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 120
 port hybrid untagged vlan 120
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 110
 port hybrid untagged vlan 110
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.0
#
nqa test-instance test jitter
 test-type jitter
 destination-address ipv4 30.1.1.2
 destination-port 9000
 threshold rtd 20
 send-trap rtd
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100007B29
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap address udp-domain 20.1.1.2 params securityname
public v2c
 snmp-agent trap enable
#
return
```

- Configuration file of Switch B

```
#
 sysname SwitchB
#
vlan batch 120 130
#
interface Vlanif120
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif130
 ip address 30.1.1.1 255.255.255.0
```

```
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 120
 port hybrid untagged vlan 120
#
interface XGigabitEthernet0/0/2
 port hybrid pvid vlan 130
 port hybrid untagged vlan 130
#
ospf 1
 area 0.0.0.1
  network 10.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```

- Configuration file of Switch C

```
#
 sysname SwitchC
#
vlan batch 130
#
interface Vlanif130
 ip address 30.1.1.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port hybrid pvid vlan 130
 port hybrid untagged vlan 130
#
  nqa-server udpecho 30.1.1.2 9000
#
ospf 1
 area 0.0.0.1
  network 30.1.1.0 0.0.0.255
#
return
```

9.7 RMON Configuration

This chapter describes how to monitor the Ethernet interface through Remote Network Monitoring (RMON).

9.7.1 Examples for Configuring RMON

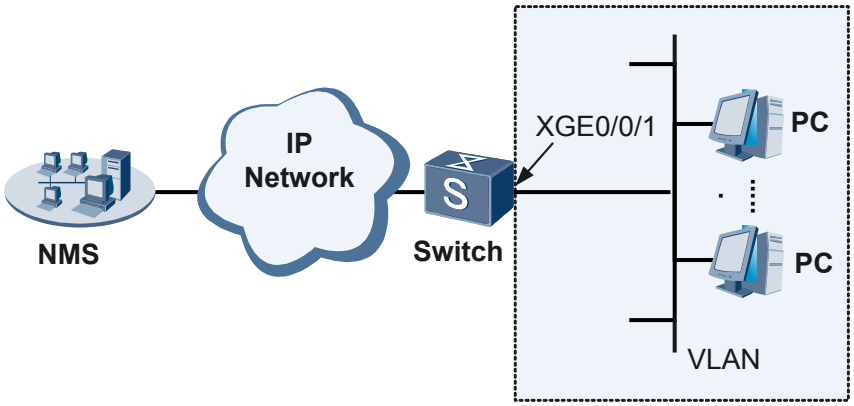
Networking Requirements

XGigabitEthernet0/0/1 on the Switch belongs to a VLAN.

As shown in **Figure 9-33**, it is required that the network connected to XGigabitEthernet0/0/1 be monitored to obtain real-time and history statistics of broadcast, multicast, and unknown unicast packets on the network.

If the number of broadcast, multicast, and unknown unicast packets in the VLAN becomes abnormal, the Switch sends a Trap message to the NMS.

Figure 9-33 Networking diagram of configuring RMON



Configuration Roadmap

To send a Trap message to the NMS, you need to use SNMP commands to enable the Trap function and set a corresponding community name. For details, refer to the chapter SNMP Configuration.

The configuration roadmap is as follows:

- Enable the statistics function.
- Configure the etherStatsTable.
- Configure the historyControlTable.
- Configure the eventTable.
- Configure the alarmTable.

Data Preparation

To complete the configuration, you need the following data:

- Interval for sampling data
- Threshold for triggering alarms
- Community name for communicating with the NMS

Configuration Procedure

1. Configure reachable routes between the Switch and the NMSs. The configuration procedure is not mentioned.
2. Enable the statistics function.

   # Enable the RMON statistics function on the interface.

   ```
   <Switch> system-view
   [Switch] interface xgigabitethernet 0/0/1
   [Switch-XGigabitEthernet0/0/1] rmon-statistics enable
   ```

   # Configure the etherStatsTable.

   ```
   [Switch-XGigabitEthernet0/0/1] rmon statistics 1 owner User01
   ```

   # Verify the configuration. You can check the traffic on the subnet.

   ```
   [Switch-XGigabitEthernet0/0/1] display rmon statistics XGigabitEthernet0/0/1
   ```

```
Statistics entry 1 owned by User01 is VALID.Received  :
  Interface : XGigabitEthernet0/0/1<ifEntry.514>
  octets              :156       , packets          :1
  broadcast packets   :0         , multicast packets:1
  undersized packets  :0         , oversized packets:0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):0
  Packets received according to length (octets):
  64     :0         ,  65-127  :0         ,  128-255  :1
  256-511:0         ,  512-1023:0         ,  1024-1518:0
```

3. # Configure Switch.

   # Sample the traffic on the subnet every 30 seconds and save the latest 10 history entries.

   ```
   [Switch-XGigabitEthernet0/0/1] rmon history 1 buckets 10 interval 30 owner
   User01
   ```

   # Verify the configuration. Only the last sampling record is displayed through CLI. To display all the history records, use the special NMS software.

   ```
   [Switch-XGigabitEthernet0/0/1] quit
   [Switch] display rmon history XGigabitEthernet0/0/1
   History control entry 1 owned by User01 is VALID
     Samples interface     : XGigabitEthernet0/0/1<ifEntry.514>
     Sampling interval     : 30(sec) with 10 buckets max
     Last Sampling time    : 0days 01h:56m:21s
     Latest sampled
   values :
     octets               :11385     , packets           :
   0
     broadcast packets    :0         , multicast packets :
   9
     undersize packets    :0         , oversize packets  :
   0
     fragments packets    :0         , jabbers packets   :
   0
     CRC alignment errors :0         , collisions        :
   0
     Dropped packet:      :0         , utilization       :
   0
     History
   record:
     Record No.1 (Sample time: 1days 07h:37m:
   29s)
     octets               :11182     , packets           :
   0
     broadcast packets    :0         , multicast packets :
   8
     undersize packets    :0         , oversize packets  :
   0
     fragments packets    :0         , jabbers packets   :
   0
     CRC alignment errors :0         , collisions        :
   0
     Dropped packet:      :0         , utilization       :0
   ```

4. Configure the eventTable.

   # Set the device to record logs for RMON event 1.

   ```
   [Switch] rmon event 1 description logevent log owner User01
   ```

   # Set the device to send Trap messages to the NMS for RMON event 2 and set the community name to public.

   ```
   [Switch] rmon event 2 description prialarmevent trap public owner User01
   ```

   # Display the alarms.

   ```
   [Switch] display rmon event
   Event table 1 owned by User01 is VALID.
     Description: logevent.
   ```

```
  Will cause log when triggered, last triggered at 0days 00h:00m:00s.
Event table 2 owned by User01 is VALID.
  Description: prialarmevent.
  Will cause snmp-trap when triggered, last triggered at 0days 00h:00m:00s.
```

5. Configure the alarmTable for broadcast packets.

   # Sample the broadcast packets every 30 seconds. Trigger event 1 when 10000 or more broadcast packets are received. Trigger event 2 when 100 broadcast or less broadcast packets are received.

   ```
   [Switch] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold
   10000 2 falling-threshold 100 1 owner User01
   ```

   # Display the alarms.

   ```
   [Switch] display rmon alarm 1
   Alarm table 1 owned by User01 is VALID.
     Samples  absolute value : 1.3.6.1.2.1.16.1.1.1.6.1<etherStatsBroadcastPkts.
   1>
     Sampling interval         : 30(sec)
     Rising threshold          : 10000(linked with event 2)
     Falling threshold         : 100(linked with event 1)
     When startup enables      : risingOrFallingAlarm
     Latest value              : 0
   ```

6. Configure the alarmTable for multicast packets.

   # Sample the multicast packets every 30 seconds. Trigger event 1 when 50000 or more multicast packets are received. Trigger event 2 when 100 or less multicast packets are received.

   ```
   [Switch] rmon alarm 2 1.3.6.1.2.1.16.1.1.1.7.1 30 absolute rising-threshold
   50000 2 falling-threshold 100 1 owner User01
   ```

   # Display the alarms.

   ```
   [Switch] display rmon alarm 2
   Alarm table 2 owned by User01 is VALID.
     Samples  absolute value : 1.3.6.1.2.1.16.1.1.1.7.1<etherStatsMulticastPkts.
   1>
     Sampling interval         : 30(sec)
     Rising threshold          : 50000(linked with event 2)
     Falling threshold         : 100(linked with event 1)
     When startup enables      : risingOrFallingAlarm
     Latest value              : 0
   ```

7. Configure the alarmTable for unknown unicast packets.

   # Sample the unicast packets every 30 seconds. Trigger event 1 when 1000 or more unicast packets are received. Trigger event 2 when 10 or less unicast packets are received.

   ```
   [Switch] rmon alarm 3 1.3.6.1.2.1.2.2.1.12.898 30 absolute rising-threshold
   1000 2 falling-threshold 10 1 owner User01
   ```

   # Display the alarms.

   ```
   [Switch] display rmon alarm 3
   Alarm table 3 owned by User01 is VALID.
     Samples    absolute value : 1.3.6.1.2.1.2.2.1.12.898<ifInNUcastPkts.898>
     Sampling interval         : 30(sec)
     Rising threshold          : 1000(linked with event 2)
     Falling threshold         : 10(linked with event 1)
     When startup enables      : risingOrFallingAlarm
   Latest value              : 0
   ```

Configuration Files

```
#
sysname Switch
#
snmp-agent
 snmp-agent local-engineid 000007DB7F000001000071B6
#
```

```
interface XGigabitEthernet0/0/1
 rmon-statistics enable
 rmon statistics 1 owner user01
 rmon history 1 buckets 10 interval 30 owner user01
#
 rmon event 1 description logevent log owner User01
 rmon event 2 description prialarmeven trap public owner User01
 rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 10000 2 falling-
threshold 100 1 owner User01
 rmon alarm 2 1.3.6.1.2.1.16.1.1.1.7.1 30 absolute rising-threshold 50000 2 falling-
threshold 100 1 owner User01
 rmon alarm 3 1.3.6.1.2.1.2.2.1.12.898 30 absolute rising-threshold 1000 2 falling-
threshold 10 1 owner User01
#
return
```