HP 7500 Switch Series

Configuration Examples

Part Number: 5998-4952

Contents

802.1X configuration examples

This chapter provides examples for configuring 802.1X authentication to control network access of LAN access users.

Example: Configuring RADIUS-based 802.1X authentication (non-IMC server)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

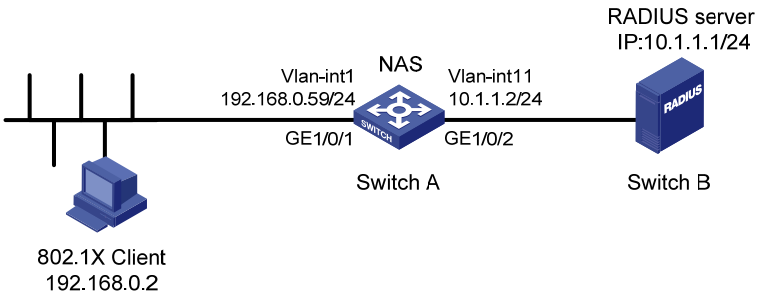
Network requirements

As shown in Figure 1:

- Users must pass 802.1X authentication to access the Internet, and they use the HP iNode client to initiate 802.1X authentication.
- Switch A uses a RADIUS server (Switch B) to perform RADIUS-based 802.1X authentication and authorization.
- The HP 5500 HI switch functions as the RADIUS server.

Configure GigabitEthernet 1/0/1 to implement MAC-based access control so each user is separately authenticated. When a user logs off, no other online users are affected.

Figure 1 Network diagram



Configuration restrictions and guidelines

When you configure RADIUS-based 802.1X authentication, follow these restrictions and guidelines:

- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS

authentication server. Configure the port used for RADIUS authentication to 1645 for the RADIUS scheme on the access device.

- Enable 802.1X globally only after you have configured the authentication-related parameters. Otherwise, users might fail to pass 802.1X authentication.
- The 802.1X configuration takes effect on a port only after you enable 802.1X globally and on the port.

Configuration procedures

Configuring IP addresses

Assign an IP address to each interface as shown in Figure 1. Make sure the client, Switch A, and the RADIUS server can reach each other. (Details not shown.)

Configuring Switch A

1. Configure the RADIUS scheme:

   # Create RADIUS scheme **radius1** and enter RADIUS scheme view.

   ```
   [SwitchA] radius scheme radius1
   New Radius scheme
   [SwitchA-radius-radius1]
   ```

   # Specify the RADIUS server at **10.1.1.1** as the primary authentication server, set the authentication port to **1645**, and specify the shared key as **abc**.

   ```
   [SwitchA-radius-radius1] primary authentication 10.1.1.1 1645 key abc
   ```

   # Exclude the ISP domain name from the username sent to the RADIUS server.

   ```
   [SwitchA-radius-radius1] user-name-format without-domain
   ```

   NOTE:

   The access device must use the same username format as the RADIUS server. If the RADIUS server includes the ISP domain name in the username, so must the access device.

   # Set the source IP address for outgoing RADIUS packets to **10.1.1.2**.

   ```
   [SwitchA-radius-radius1] nas-ip 10.1.1.2
   [SwitchA-radius-radius1] quit
   ```

2. Configure the ISP domain:

   # Create ISP domain **test** and enter ISP domain view.

   ```
   [SwitchA] domain test
   [SwitchA-isp-test]
   ```

   # Configure ISP domain **test** to use RADIUS scheme **radius1** for authentication and authorization of all 802.1X users.

   ```
   [SwitchA-isp-test] authentication lan-access radius-scheme radius1
   [SwitchA-isp-test] authorization lan-access radius-scheme radius1
   [SwitchA-isp-test] quit
   ```

   # Specify domain **test** as the default ISP domain. If a user does not provide any ISP domain name, it is assigned to the default ISP domain.

   ```
   [SwitchA] domain default enable test
   ```

3. Configure 802.1X:

   # Enable 802.1X on port GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] dot1x
 802.1x is enabled on port GigabitEthernet1/0/1.
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/1 to implement MAC-based access control. This step is optional, because the port implements MAC-based access control by default.

```
[SwitchA] dot1x port-method macbased interface gigabitethernet 1/0/1
```

Enable 802.1X globally.

```
[SwitchA] dot1x
 802.1x is enabled globally.
```

Configuring the RADIUS server

Create RADIUS user **guest** and enter RADIUS server user view.

```
<Sysname> system-view
[Sysname] radius-server user guest
[Sysname-rdsuser-guest]
```

Set the password to **123456** in plain text for RADIUS user **guest**.

```
[Sysname-rdsuser-guest] password simple 123456
[Sysname-rdsuser-guest] quit
```

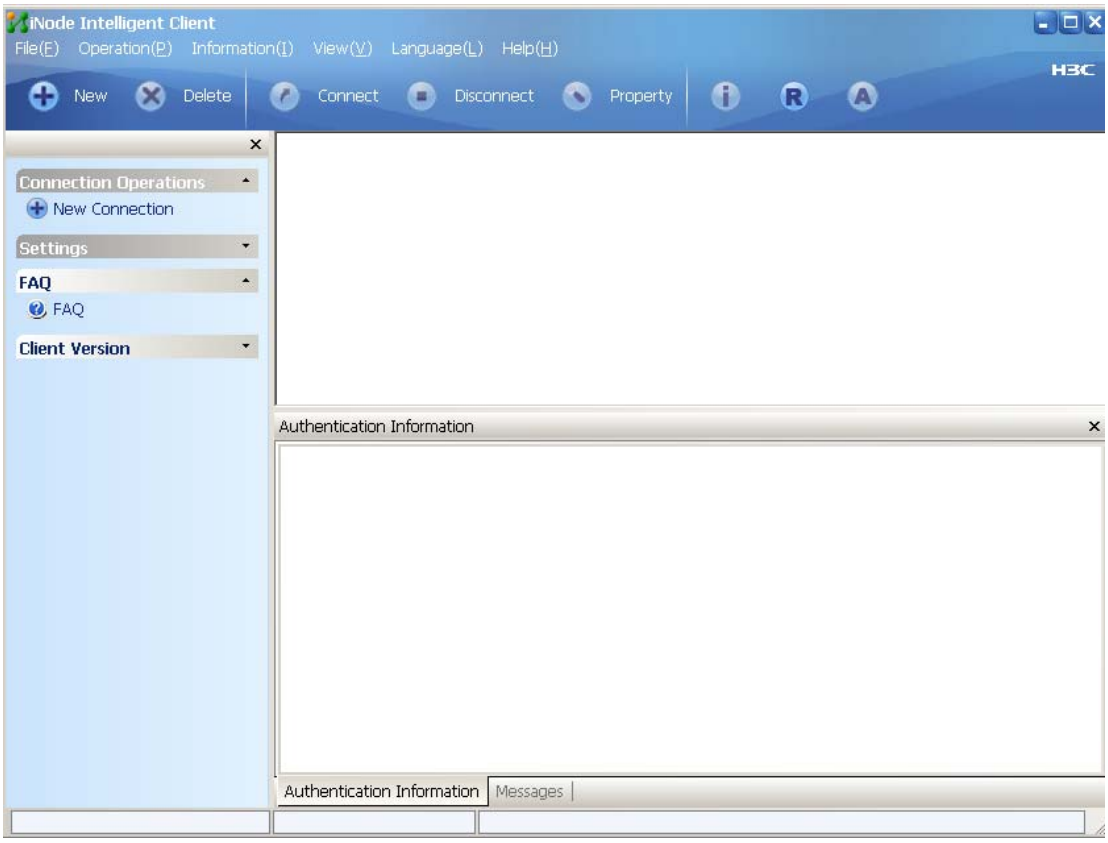
Specify RADIUS client **10.1.1.2**, and set the shared key to **abc** in plain text.

```
[Sysname] radius-server client-ip 10.1.1.2 key simple abc
```

Configuring the 802.1X client

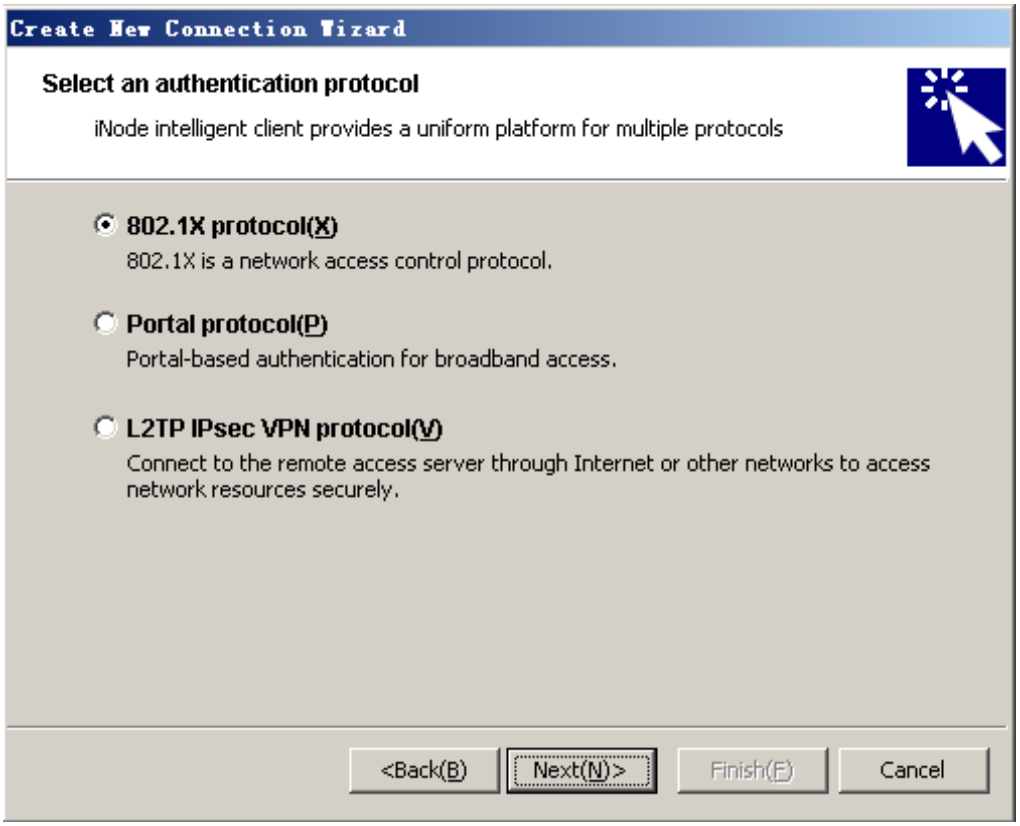
1. Open the iNode client as shown in Figure 2.

Figure 2 Opening iNode client



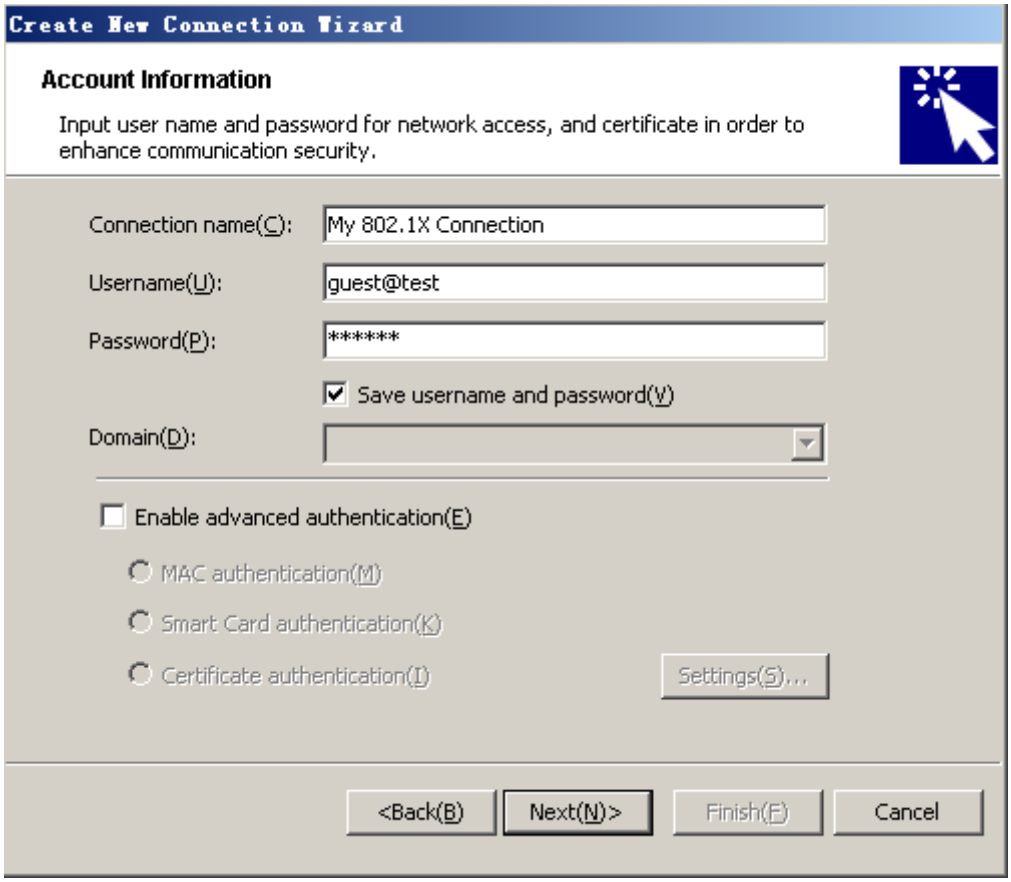
2. Click **New**.
3. On the **Create New Connection Wizard** window, select **802.1X protocol(X)**, and then click **Next(N)>**.

Figure 3 Creating a new connection



4. Configure the connection name, username, and password, and then click **Next(N)>**.

Figure 4 Configuring the connection name, username, and password



The following details must comply with the correlation rules shown in Table 1:

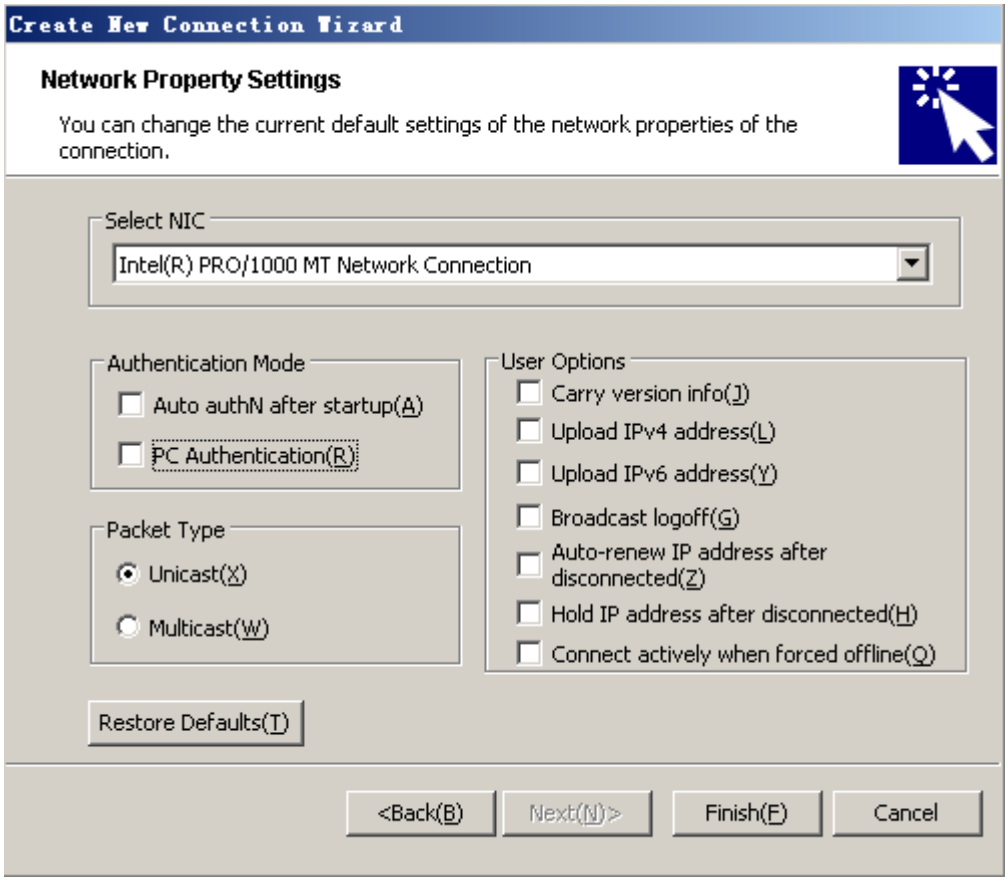
- The username specified on the iNode client.
- The domain and RADIUS scheme configuration on the access device.
- The suffix of the service on the UAM.

Table 1 Parameter correlation

Username format on the iNode client	Domain on the access device	Username format configured on the access device	Service suffix on UAM
X@Y	Y	with-domain	Y
X@Y	Y	without-domain	No suffix
X	Default domain (the default domain specified on the access device)	with-domain	Name of the default domain
X	Default domain (the default domain specified on the access device)	without-domain	No suffix

5. Configure the connection properties.

Figure 5 Configuring 802.1X connection properties



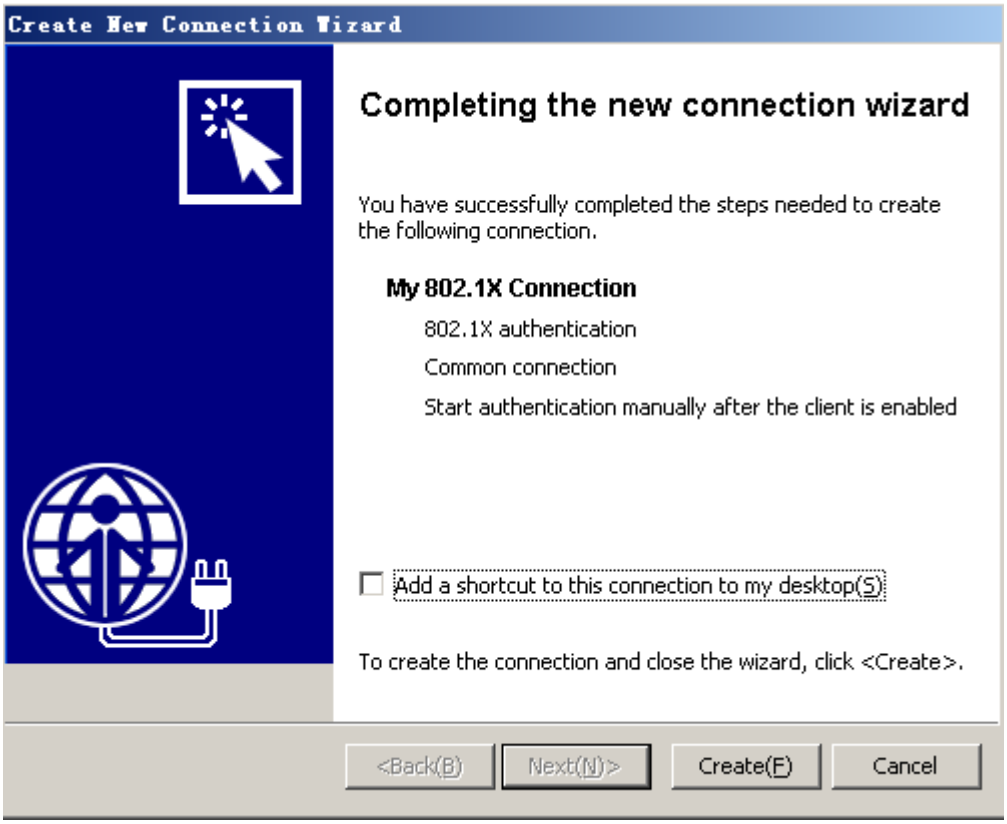
a. If you select the **Carry version info(J)** item in the **User Options** area, the 802.1X client adds the client version number to the EAP packets that are sent to the UAM for 802.1X authentication.

b. If you do not select this item, the 802.1X client sends standard EAP packets to the UAM for 802.1X authentication.

c. Do not select this item if you set local authentication as the backup authentication method, because the access device cannot recognize the version number.

6. Click **Create(F)**.

Figure 6 Completing the new connection wizard



7. Click **Connect** on the iNode client to initiate the connection.
8. Enter the correct username and password, select **Save username and password(D)**, and click **Connect(C)**.

Figure 7 Initiating the 802.1X connection

Configuration files

- Switch A (the access device):

```
#
domain default enable test
#
 dot1x
#
radius scheme radius1
 primary authentication 10.1.1.1 1645 key cipher
$c$3$I9rdLmT82kyz1eyzYDZv46s+V4r0Bw==
 user-name-format without-domain
 nas-ip 10.1.1.2
#
domain test
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 access-limit disable
 state active
self-service-url disable
#
interface Vlan-interface1
 ip address 192.168.0.59 255.255.255.0
#
interface Vlan-interface11
```

```
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 11
#
```

- Switch B (the RADIUS server):

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$EEKWoSNy6Om3tZ0PhUbTPLuWMY2+aw==
#
radius-server user guest
 password cipher $c$3$4rJuGA/vjrZHO+o33+/NPkcVZWuY8nnDzw==
#
interface Vlan-interface11
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/10
 port access vlan 11
#
```

Example: Configuring RADIUS-based 802.1X authentication (IMC server)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

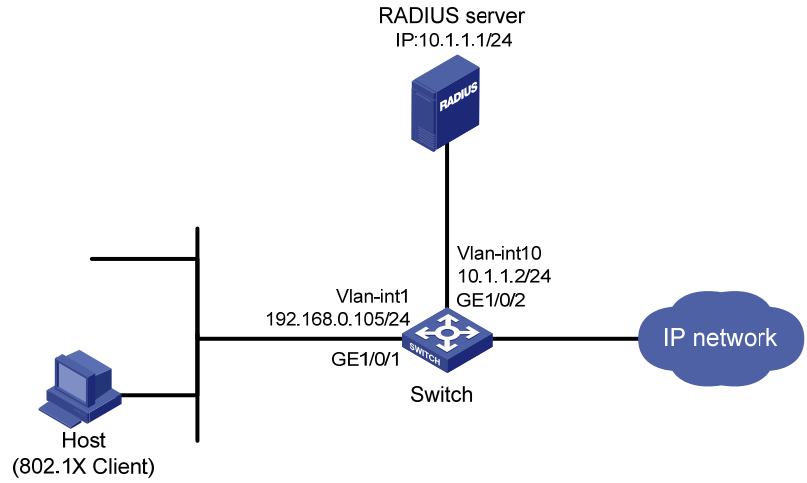
Network requirements

As shown in Figure 8:

- The host must pass 802.1X authentication to access the network, and the host uses HP iNode client to initiate 802.1X authentication.
- The switch uses the IMC server to perform RADIUS-based 802.1X authentication.
- If a user passes RADIUS 802.1X authentication, it can access to the IP network.

Configure GigabitEthernet 1/0/1 to implement MAC-based access control so each user is separately authenticated. When a user logs off, no other online users are affected.

Figure 8 Network diagram



Configuration restrictions and guidelines

The RADIUS server in this example runs on IMC PLAT 5.2 (E0401) and IMC UAM 5.2 (E0402). The configuration examples vary with IMC versions, deployed service components, and UAM system settings. For more information, see *HP IMC User Access Manager Administrator Guide*.

Configuration procedures

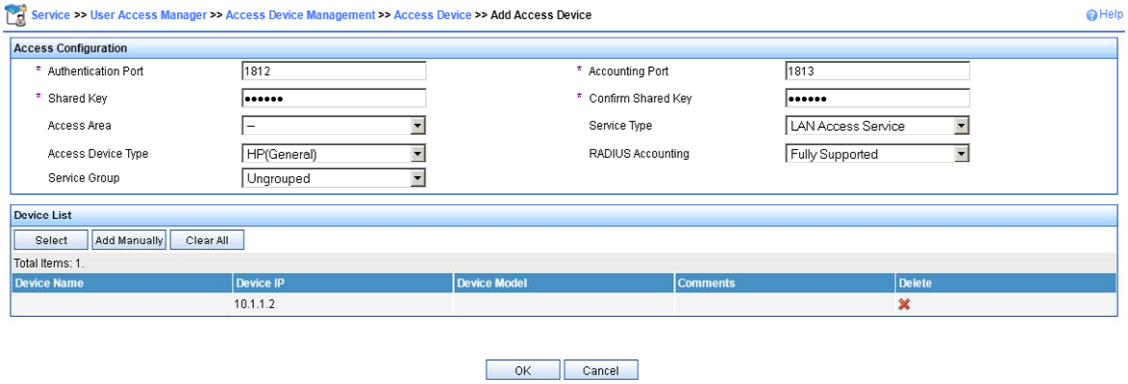
Configuring IP addresses

Configure the IP addresses for interfaces as shown in Figure 8, and make sure the host, server, and switch can reach each other. (Details not shown.)

Configuring the RADIUS server

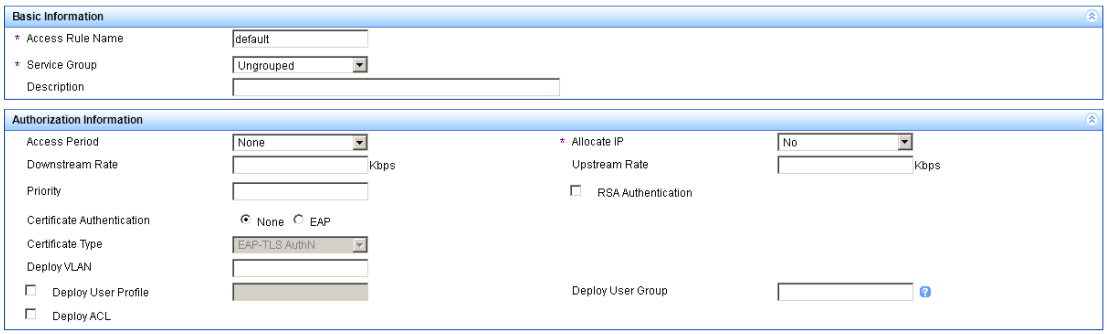
1. Add the switch to IMC as an access device:
   a. Click the **Service** tab.
   b. Select **User Access Manager** > **Access Device Management** > **Access Device** from the navigation tree.
   c. Click **Add**.
   d. In the **Access Configuration** area, configure the following parameters:
      – Enter **1812** in the **Authentication Port** field.
      – Enter **1813** in the **Accounting Port** field.
      – Enter **aabbcc** in **Shared Key** and **Confirm Shared Key** fields.
      – Select **LAN Access Service** from the **Service Type** list.
      – Select **HP(General)** from the **Access Device Type** list.
      – Use the default settings for other parameters.
   e. On the **Device List**, click **Select** or **Add Manually** to specify 10.1.1.2 as the device IP address.
   f. Click **OK**.

Figure 9 Adding an access device in IMC



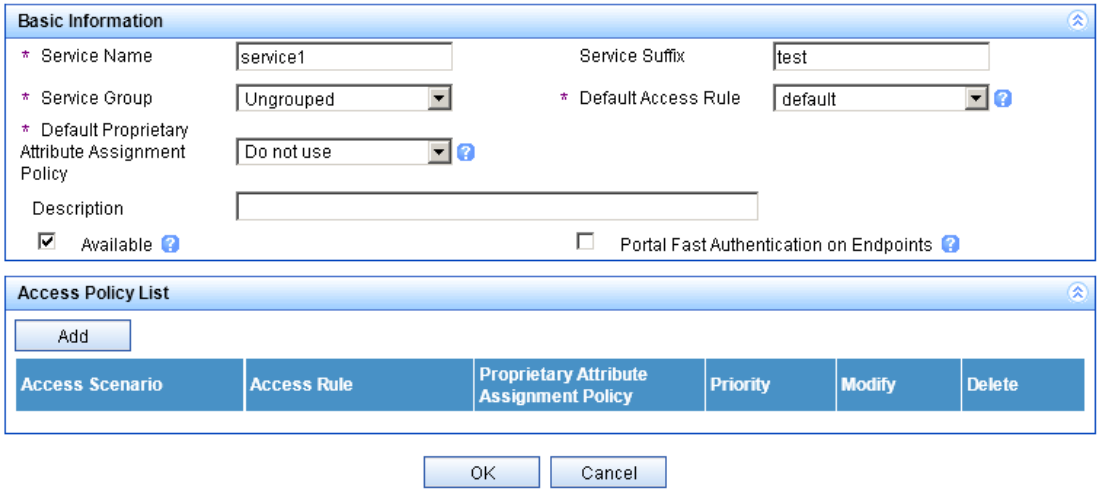
2. Add an access rule:
   a. Click the **Service** tab.
   b. Select **User Access Manager** > **Access Rule Management** from the navigation tree.
   c. Click **Add**.
   d. Enter **default** in the **Access Rule Name** field, and use the default settings for other parameters.
   e. Click **OK**.

Figure 10 Adding an access rule in IMC



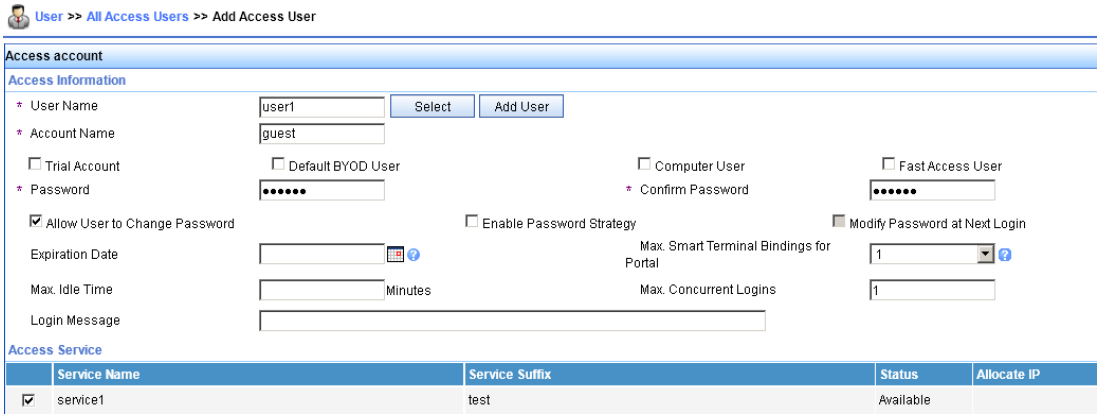
3. Add a service:
   a. Click the **Service** tab.
   b. Select **User Access Manager** > **Service Configuration** from the navigation tree.
   c. Click **Add**.
   d. In the **Basic Information** area, configure the following parameters:
      – Enter **service1** in the **Service Name** field.
      – Enter **test** in the **Service Suffix** field. For more information about the service suffix, see Table 1.
      – Select **default** from the **Default Access Rule** list.
      – Use the default settings for other parameters.
   e. Click **OK**.

Figure 11 Adding a service in IMC



4. Add an access user account and assign the service to the account:
   a. Click the **User** tab.
   b. Select **Access User View** > **All Access Users** from the navigation tree.
   c. Click **Add**.
   d. In the **Access Information** area, click **Add User** to create a Platform user named **user1**.
   e. Configure the following parameters:
      – Enter **guest** in the **Account Name** field to identify the 802.1X user.
      – Enter **123456** in **Password** and **Confirm Password** fields.
      – Use the default settings for other parameters.
   f. In the **Access Service** area, select **service1** on the list.
   g. Click **OK**.

Figure 12 Adding an access user account in IMC



Configuring the switch

Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1]
```

Specify the RADIUS server at **10.1.1.1** as the primary authentication server.

```
[Switch-radius-radius1] primary authentication 10.1.1.1
```

Set the shared key for authentication to **aabbcc**.

```
[Switch-radius-radius1] key authentication aabbcc
```

Configure the RADIUS server type of RADIUS scheme **radius1** as **extended**.

```
[Switch-radius-radius1] server-type extended
```

Set the response timeout time of the RADIUS server to 5 seconds. Set the maximum number of RADIUS packet retransmission attempts to 5.

```
[Switch-radius-radius1] timer response-timeout 5
[Switch-radius-radius1] retry 5
[Switch-radius-radius1] quit
```

Create an ISP domain named **test** and enter ISP domain view.

```
[Switch] domain test
[Switch-isp-test]
```

Configure ISP domain **test** to use RADIUS scheme **radius1** as the primary authentication and authorization method for 802.1X users.

```
[Switch-isp-test] authentication lan-access radius-scheme radius1
[Switch-isp-test] authorization lan-access radius-scheme radius1
```

Enable the idle cut function, and set the idle timeout period to 20 minutes.

```
[Switch-isp-test] idle-cut enable 20
[Switch-isp-test] quit
```

Specify domain **test** as the default ISP domain.

```
[Switch] domain default enable test
```

Enable 802.1X on port GigabitEthernet 1/0/1.

```
[Switch] interface gigabitthernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet 1/0/1 to implement MAC-based access control. This task is optional, because the port by default implements MAC-based access control.

```
[Switch] dot1x port-method macbased interface gigabitethernet 1/0/1
```

Enable 802.1X globally.

```
[Switch] dot1x
```

Configuring the 802.1X client

Use an HP iNode client to create 802.1X connections (see "Example: Configuring RADIUS-based 802.1X authentication (non-IMC server)").

Verifying the configuration

Click **Connect** on the iNode client, enter username **guest@test** and password **123456** on the **My 802.1X Connection** window, and then Click **Connect(C)**.

The user can pass 802.1X authentication and access the Internet.

Configuration files

```
#
 domain default enable test
#
 dot1x
#
vlan 1
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
 timer response-timeout 5
 retry 5
#
domain test
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 access-limit disable
 state active
 idle-cut enable 20 10240
 self-service-url disable
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
#
```

Example: Configuring 802.1X unicast trigger

If a client cannot send EAPOL-Start packets, you can configure the access device to initiate authentication. For example, if the 802.1X client available with Windows XP exists in the network, configure the access device to initiate the 802.1X authentication.

The access device supports the following modes:

- **Multicast trigger mode**—The access device multicasts Identity EAP-Request packets periodically (every 30 seconds by default) to initiate 802.1X authentication.
- **Unicast trigger mode**—The access device sends an Identity EAP-Request packet to the unknown MAC address when it receives a frame with the source MAC address not in the MAC address table. It retransmits the packet if no response has been received within a certain time interval.

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

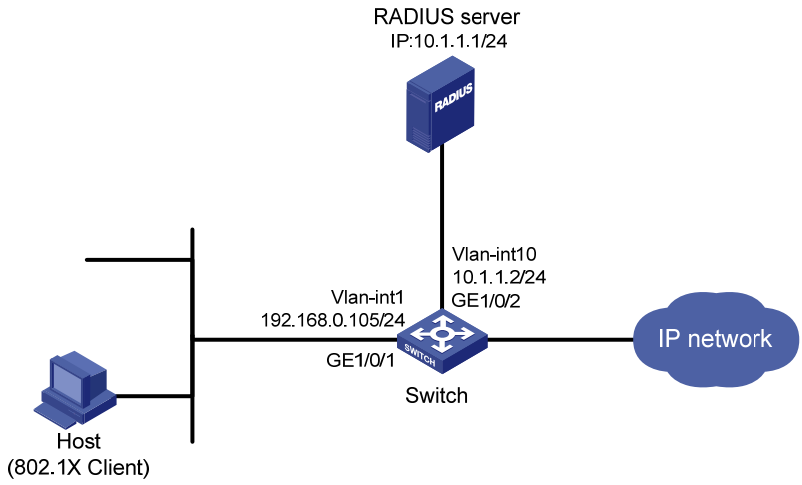
Network requirements

As shown in Figure 13, the host must pass 802.1X authentication to access the network, and a RADIUS IMC server is available for authentication and authorization of 802.1X users.

Configure GigabitEthernet 1/0/1 to implement MAC-based access control so each user is separately authenticated. When a user logs off, no other online users are affected.

- The host uses the built-in 802.1X client of Windows XP. 802.1X unicast trigger is enabled on GigabitEthernet 1/0/1 of the switch to initiate 802.1X authentication.
- The switch does not multicast Identity EAP-Request packets periodically.

Figure 13 Network diagram



Configuration restrictions and guidelines

In multicast trigger mode, the access device multicasts a large number of Identity EAP-Request packets periodically to the host, which consumes bandwidth and system resources. HP recommends disabling the 802.1X multicast trigger function when you enable the unicast trigger function.

Configuration procedures

Configuring interfaces

Configure interfaces, and assign IP addresses to interfaces, as shown in Figure 13. Make sure the host, switch, and server can reach each other. (Details not shown.)

Configuring the RADIUS server

See "Example: Configuring RADIUS-based 802.1X authentication (IMC server)."

Configuring the access device

Create RADIUS scheme **radius1** and enter RADIUS scheme view.

```
<Switch> system-view
[Switch] radius scheme radius1
[Switch-radius-radius1]
```

Specify the RADIUS server at **10.1.1.1** as the primary authentication server.

```
[Switch-radius-radius1] primary authentication 10.1.1.1
```

Set the shared key for authentication to **aabbcc**.

```
[Switch-radius-radius1] key authentication aabbcc
```

Configure the RADIUS server type of RADIUS scheme **radius1** as **extended**.

```
[Switch-radius-radius1] server-type extended
[Switch-radius-radius1] quit
```

Create ISP domain **test** and enter ISP domain view.

```
[Switch] domain test
```

Configure ISP domain **test** to use RADIUS scheme **radius1** as primary authentication and authorization method.

```
[Switch-isp-test] authentication lan-access radius-scheme radius1
[Switch-isp-test] authorization lan-access radius-scheme radius1
[Switch-isp-test] quit
```

Specify domain **test** as the default ISP domain.

```
[Switch] domain default enable test
```

Disable the 802.1X multicast trigger function for port GigabitEthernet 1/0/1.

```
[Switch] interface gigabitthernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo dot1x multicast-trigger
```

Enable the 802.1X unicast trigger function on the port.

```
[Switch-GigabitEthernet 1/0/1] dot1x unicast-trigger
```

Enable 802.1X on the port.

```
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

Configure the port to implement MAC-based access control. This step is optional, because the port by default implements MAC-based access control.

```
[Switch] dot1x port-method macbased interface gigabitethernet 1/0/1
```

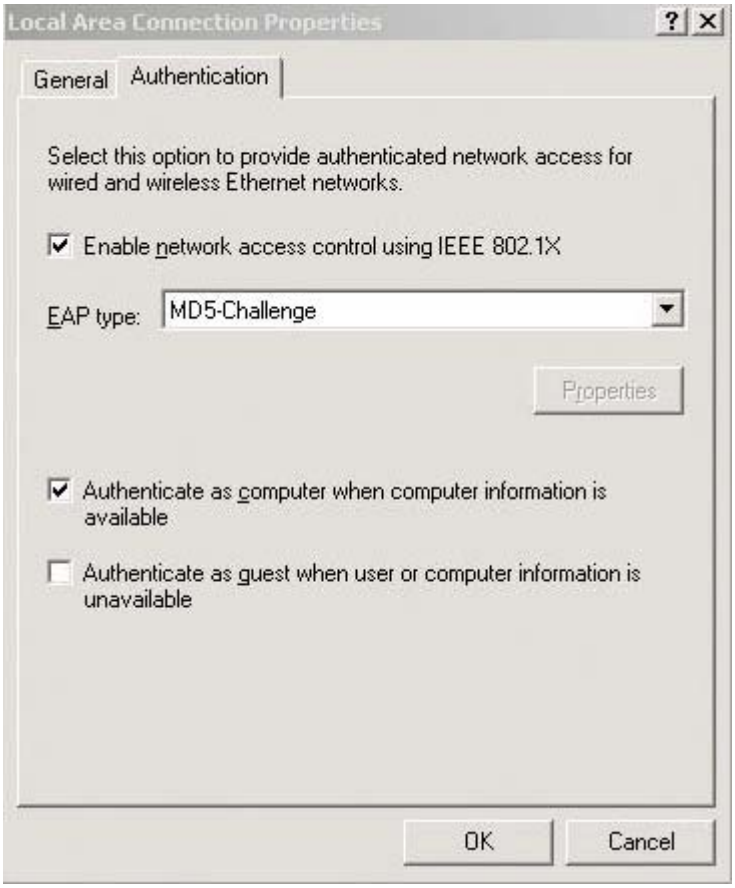
Enable 802.1X globally.

```
[Switch] dot1x
```

Configuring the 802.1X client

On the **Local Area Connection Properties** window, enable 802.1X authentication for the Windows XP system, as shown in Figure 14.

Figure 14 Enabling 802.1X authentication for the Windows XP system



Verifying the configuration

Use the host to visit an Internet Webpage. Enter username **guest@test** and password **123456**.

Configuration files

```
#
 domain default enable test
#
 dot1x
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
 key authentication $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication default radius-scheme radius1
 authorization default radius-scheme radius1
 access-limit disable
 state active
 idle-cut disable
```

```
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 undo dot1x multicast-trigger
 dot1x
 dot1x unicast-trigger
#
```

Example: Configuring 802.1X Auth-Fail VLAN and VLAN assignment

Applicable product matrix

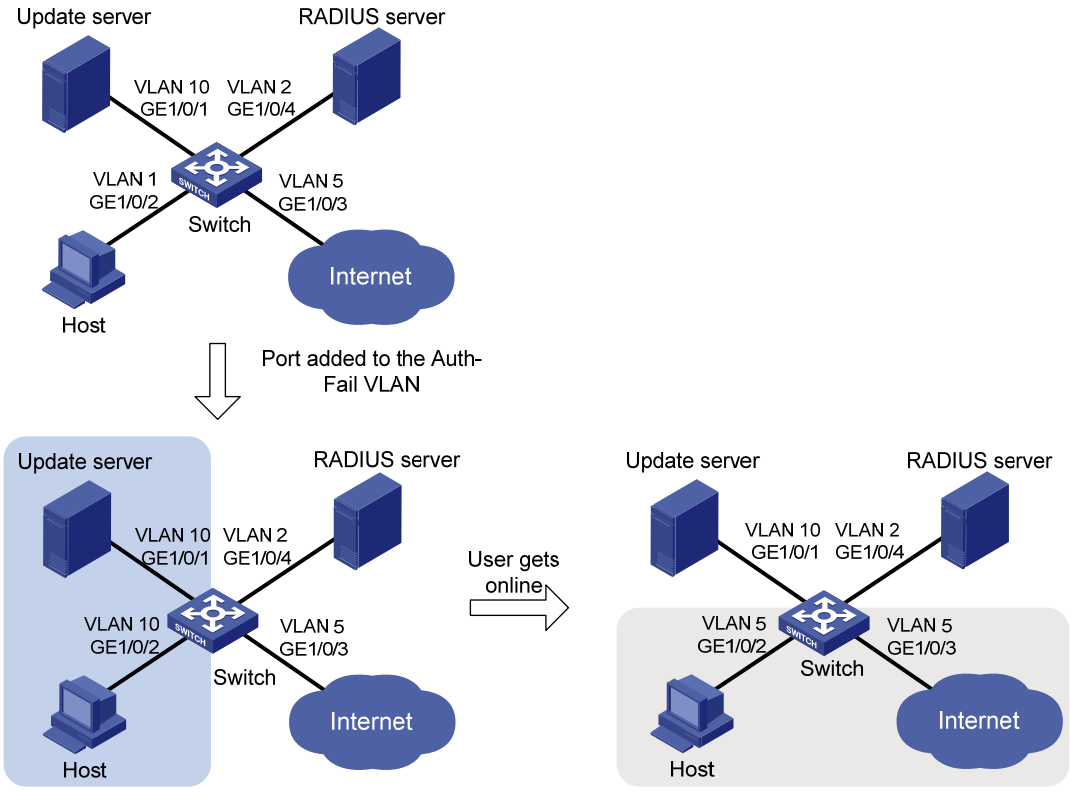
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 15:

- The host in VLAN 1 must pass 802.1X authentication to access the Internet. A RADIUS server is available and in VLAN 2.
- GigabitEthernet 1/0/3 that is connected to the Internet is assigned to VLAN 5.
- The update server in VLAN 10 is for client software download and upgrade.
- After a user fails to pass 802.1X authentication on port GigabitEthernet 1/0/2, the user can visit the update server but Internet.
- After the user passes 802.1X authentication, it can access the Internet.

Figure 15 Network diagram



Requirements analysis

After a user fails to pass 802.1X authentication on port GigabitEthernet 1/0/2, the user can visit the update server in VLAN 10, so GigabitEthernet 1/0/2 must be assigned to VLAN 10. To assign the port to VLAN 10 after the user failing to pass 802.1X authentication, you must configure VLAN 10 as the 802.1X Auth-Fail VLAN for the port.

To make sure an 802.1X user can access the Internet, you must configure the RADIUS server to assign GigabitEthernet 1/0/2 to VLAN 5 after the user passes authentication.

Configuration restrictions and guidelines

When you configure 802.1X Auth-Fail VLAN, follow these restrictions and guidelines:

- To make sure the port can correctly process VLAN tagged incoming traffic, assign different IDs to the following VLANs:
  - The voice VLAN.
  - The port VLAN.
  - The 802.1X Auth-Fail VLAN on the port.
- You cannot specify a VLAN as both a super VLAN and an 802.1X Auth-Fail VLAN.

Configuration procedures

Configuring the RADIUS server

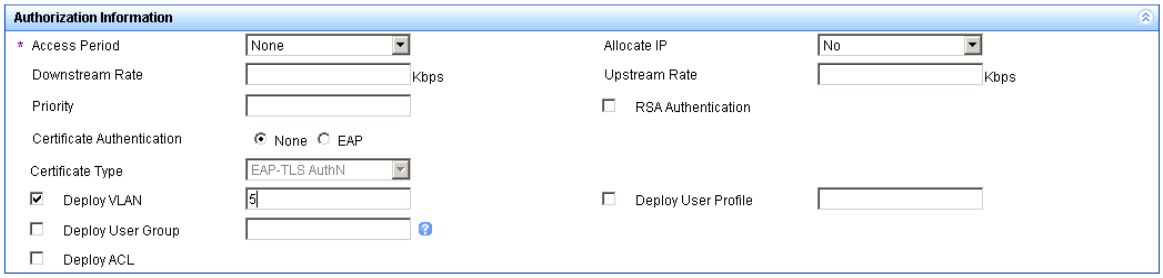
Configure the IMC server in the same way the server is configured in "Example: Configuring RADIUS-based 802.1X authentication (IMC server)," except for adding an access rule.

To add an access rule:

1. Click the **Service** tab.
2. Select **User Access Manager** > **Access Rule Management** from the navigation tree.
3. Click **Add**.
4. Select **Deploy VLAN**, and enter the VLAN number.

   This example uses VLAN 5 and sets the other parameters to use the default settings.
5. Click **OK**.

Figure 16 Configuring Auth-Fail VLAN



Configuring the switch

1. Configure VLANs 2, 5, and 10.

```
<Switch> system-view
[Switch] vlan 1
[Switch-vlan1] port gigabitethernet 1/0/2
[Switch-vlan1] quit
[Switch] vlan 10
[Switch-vlan10] port gigabitethernet 1/0/1
[Switch-vlan10] quit
[Switch] vlan 2
[Switch-vlan2] port gigabitethernet 1/0/4
[Switch-vlan2] quit
[Switch] vlan 5
[Switch-vlan5] port gigabitethernet 1/0/3
[Switch-vlan5] quit
```

2. Configure a RADIUS scheme:

   # Create RADIUS scheme **radius1**, and enter RADIUS scheme view.

```
[Switch] radius scheme radius1
[Switch-radius-radius1]
```

   # Specify the RADIUS server at **10.11.1.1** as the primary authentication server, set the authentication port to **1812**, and configure the shared key to **aabbcc**.

```
[Switch-radius-radius1] primary authentication 10.11.1.1 1812
[Switch-radius-radius1] key authentication aabbcc
```

Configure the RADIUS server type of RADIUS scheme **radius1** as **extended**.

```
[Switch-radius-radius1] server-type extended
```

Configure the device to send usernames to the RADIUS server with domain names.

```
[Switch-radius-radius1] user-name-format with-domain
[Switch-radius-radius1] quit
```

3. Configure the ISP domain:

Create ISP domain **test**, and enter ISP domain view.

```
[Switch] domaim test
[Switch-isp-test]
```

Configure ISP domain **test** to use RADIUS scheme **radius1** for authentication and authorization of all LAN-access users.

```
[Switch-isp-test] authentication lan-access radius-scheme radius1
[Switch-isp-test] authorization  lan-access radius-scheme radius1
[Switch-isp-test] quit
```

Specify domain **test** as the default ISP domain.

```
[Switch] domain default enable test
```

4. Configure 802.1X:

Enable 802.1X on port GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] dot1x
```

Configure the port to implement port-based access control.

```
[Switch-GigabitEthernet1/0/2] dot1x port-method portbased
```

Set the authorization state of the port to **auto**. This step is optional, because the authorization state of the port is **auto** by default.

```
[Switch-GigabitEthernet1/0/2] dot1x port-control auto
```

Configure VLAN 10 as the Auth-Fail VLAN for the port.

```
[Switch-GigabitEthernet1/0/2] dot1x auth-fail vlan 10
[Switch-GigabitEthernet1/0/2] quit
```

Enable 802.1X globally.

```
[Switch] dot1x
```

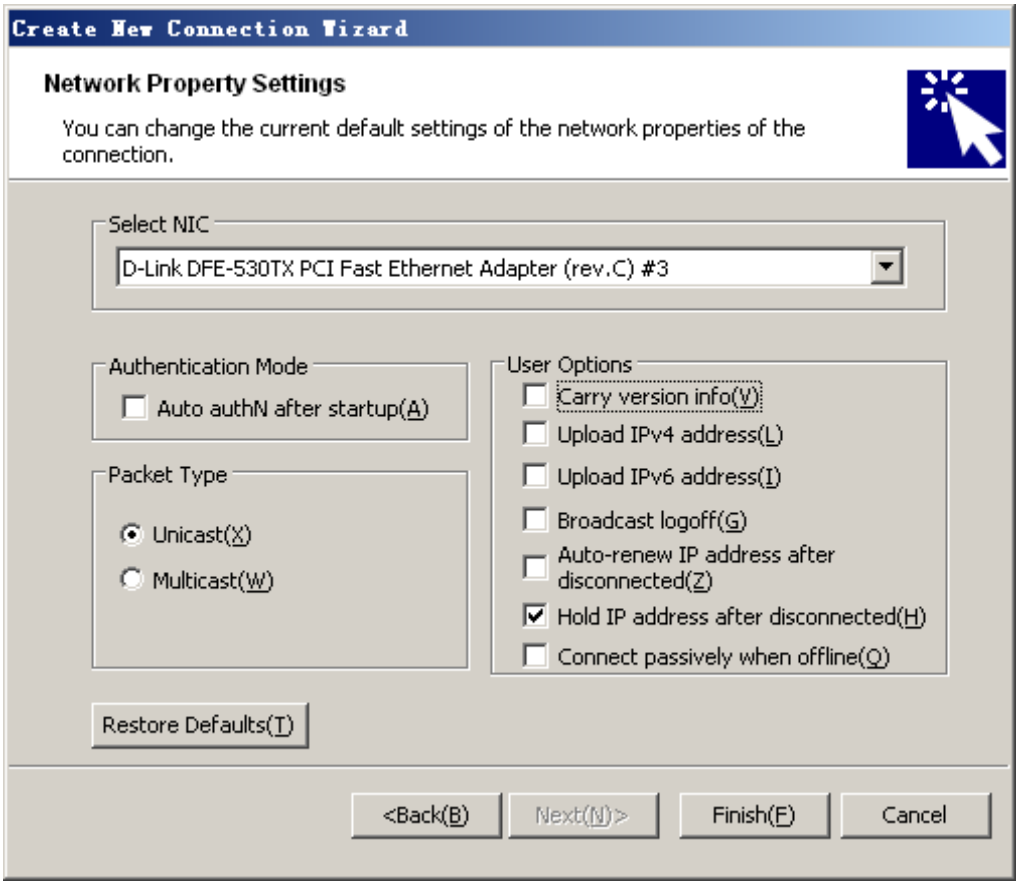
Configuring the 802.1X client

Configure the 802.1X client in the same way the client is configured in "Example: Configuring RADIUS-based 802.1X authentication (non-IMC server)," except for setting network properties.

To set 802.1X network properties:

1. Open the **Create New Connection Wizard** window.
2. Follow the steps until the **Network Property Settings** dialog box appears.
3. Select **Hold IP address after disconnected(H)** in the **User Options** area.
4. Click **Next(N)>**.

Figure 17 Configuring 802.1X network property settings



Verifying the configuration

1. Use the **display dot1x interface gigabitethernet 1/0/2** command to verify the 802.1X Auth-Fail VLAN configuration on port GigabitEthernet 1/0/2.
2. After a user fails to pass 802.1X authentication on the port, use the **display vlan 10** command to verify whether GigabitEthernet 1/0/2 is assigned to VLAN 10.
3. After the user passes authentication, use the **display interface gigabitethernet 1/0/2** command to verity that port GigabitEthernet 1/0/2 has been added to VLAN 5.

Configuration files

```
#
 domain default enable test
#
 dot1x
#
vlan 1
#
vlan 2
#
vlan 5
#
```

```
vlan 10
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 dot1x auth-fail vlan 10
 dot1x port-method portbased
 dot1x
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 2
#
```

Example: Configuring 802.1X authentication with ACL assignment

Applicable product matrix

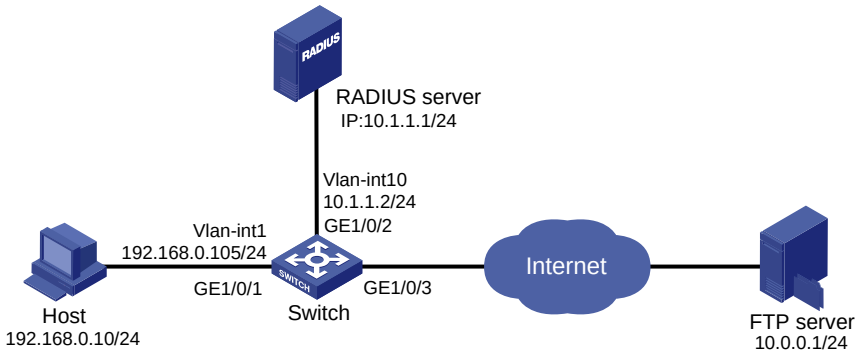
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 18, the host must pass 802.1X authentication to access the Internet. A RADIUS server is available for authentication and authorization of 802.1X users.

Assign an ACL to GigabitEthernet 1/0/1 to deny the access of 802.1X users to the FTP server at 10.0.0.1/24.

Figure 18 Network diagram



Configuration restrictions and guidelines

When you configure 802.1X authentication with ACL assignment, follow these restrictions and guidelines:

- Configure the ACL rule on the access device, and specify the ACL number on the IMC server for 802.1X users.
- You can change the access right of 802.1X users by respecifying an ACL number on the IMC server or modifying the ACL rule on the access device.
- Configure the IMC server to re-authenticate each online 802.1X user periodically for updating the access right of 802.1X users.

Configuration procedures

Configuring IP addresses

Configure IP addresses for interfaces as shown in Figure 18. Make sure the host, switch, and servers can reach each other. (Details not shown.)

Configuring the RADIUS server

Configure the IMC server in the same way the server is configured in "Example: Configuring RADIUS-based 802.1X authentication (IMC server)," except for adding an access rule.

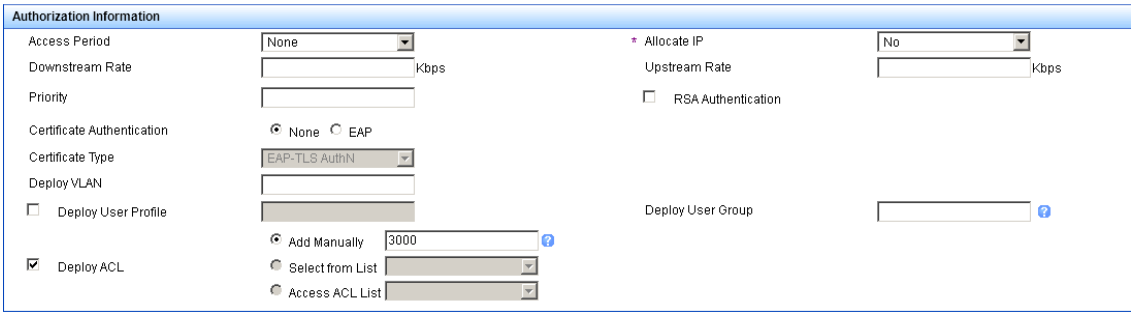
To add an access rule:

1. Click the **Service** tab.
2. Select **User Access Manager** > **Access Rule Management** from the navigation tree.
3. Click **Add**.
4. In the **Authorization Information** area, select **Deploy ACL** and **Add Manually**, and enter the ACL number.

   This example uses ACL 3000. The other parameters use the default settings.

5. Click **OK**.

Figure 19 Deploying an ACL



Configuring the switch

1. Configure the RADIUS scheme:

   # Create RADIUS scheme **radius1** and enter RADIUS scheme view.

   ```
   <Switch> system-view
   [Switch] radius scheme radius1
   [Switch-radius-radius1]
   ```

   # Specify the RADIUS server at **10.1.1.1** as the primary authentication server, and set the shared key to **aabbcc**.

   ```
   [Switch-radius-radius1] primary authentication 10.1.1.1 1812
   [Switch-radius-radius1] key authentication aabbcc
   ```

   # Configure the RADIUS server type of RADIUS scheme **radius1** as **extended**.

   ```
   [Switch-radius-radius1] server-type extended
   ```

   # Configure the device to send usernames with domain suffix.

   ```
   [Switch-radius-radius1] user-name-format with-domain
   [Switch-radius-radius1] quit
   ```

2. Configure AAA:

   # Create ISP domain **test**, and configure the domain to use RADIUS scheme **radius1** for authentication and authorization of all LAN-access users.

   ```
   [Switch] domain test
   [Switch-isp-test] authentication lan-access radius-scheme radius1
   [Switch-isp-test] authorization lan-access radius-scheme radius1
   [Switch-isp-test] quit
   ```

   # Specify domain **test** as the default ISP domain for 802.1X authentication.

   ```
   [Switch] domain default enable test
   ```

   # Configure ACL 3000 to deny packets destined for the FTP server at 10.0.0.1.

   ```
   [Switch] acl number 3000
   [Switch-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
   [Switch-acl-adv-3000] quit
   ```

3. Configure 802.1X:

   # Sets the periodic re-authentication timer to 1800 seconds.

   ```
   [Switch] dot1x timer reauth-period 1800
   ```

   # Enable the 802.1X periodic online user re-authentication function on port GigabitEthernet 1/0/1.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x re-authenticate
```

Enable 802.1X on the port.

```
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

Enable 802.1X globally.

```
[Switch] dot1x
```

Verifying the configuration

Use the user account to pass authentication, and then ping the FTP server.

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The output shows that ACL 3000 has taken effect on the user, and the user cannot access the FTP server.

Configuration files

```
#
 domain default enable test
#
 dot1x
 dot1x timer reauth-period 1800
#
acl number 3000
 rule 0 deny ip destination 10.0.0.1 0
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
```

```
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x re-authenticate
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
#
```

Example: Configuring EAD fast deployment

Applicable product matrix

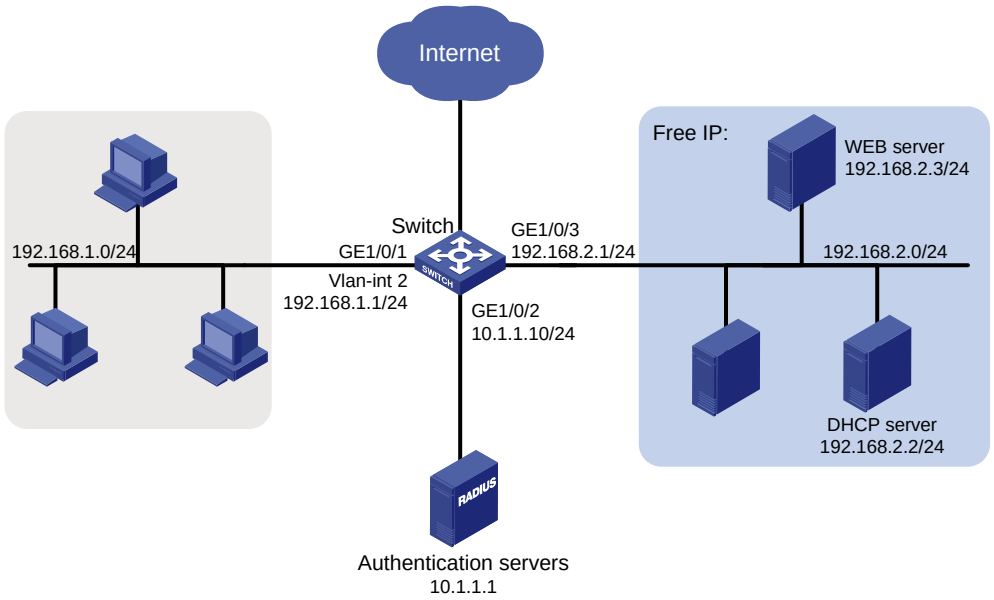
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 20, the hosts on the intranet 192.168.1.0/24 are attached to port GigabitEthernet 1/0/1 of the switch (the network access device), and they use DHCP to obtain IP addresses.

- Deploy the EAD solution for the intranet so that all hosts must pass 802.1X authentication to access the network.
- Configure the following to allow all intranet users to install and update the 802.1X client program from a Web server:
  - Allow unauthenticated users to visit the Web server and DHCP server. These users can obtain IP addresses on the segment of 192.168.1.0/24 through DHCP.
  - Redirect unauthenticated users to a preconfigured webpage when the users use a Web browser to access any external network except 192.168.2.0/24. The webpage allows users to download the 802.1X client program.
  - Allow authenticated 802.1X users to access the network.

Figure 20 Network diagram



Configuration restrictions and guidelines

When you configure EAD fast deployment, follow these restrictions and guidelines:

- Make sure you have deployed the Web server before the EAD fast deployment is configured.
- When a free IP is configured, the EAD fast deployment is enabled. To allow a user to obtain a dynamic IP address before passing 802.1X authentication, make sure the DHCP server is on the free IP segment.
- The redirect URL must be on the free IP segment.

Configuration procedures

1. Configure an IP address for each interface. (Details not shown.)
2. Configure DHCP relay:

   # Enable DHCP.

   ```
   <Switch> system-view
   [Switch] dhcp enable
   ```

   # Specify DHCP server 192.168.2.2 for the DHCP server group on the relay agent.

   ```
   [Switch] dhcp relay server-group 1 ip 192.168.2.2
   ```

   # Enable the relay agent on VLAN-interface 2.

   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] dhcp select relay
   ```

   # Correlate VLAN-interface 2 to the DHCP server group.

   ```
   [Switch-Vlan-interface2] dhcp relay server-select 1
   [Switch-Vlan-interface2] quit
   ```
3. Configure the RADIUS scheme and ISP domain.

   See "Example: Configuring RADIUS-based 802.1X authentication (IMC server)."
4. Configure 802.1X:

Configure the free IP.

```
[Switch] dot1x free-ip 192.168.2.0 24
```

Configure the redirect URL for client software download.

```
[Switch] dot1x url http://192.168.2.3
```

Enable 802.1X on port GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

Enable 802.1X globally.

```
[Switch] dot1x
```

Verifying the configuration

Use the **display dot1x** command to display the 802.1X configuration. After the host obtains an IP address from a DHCP server, use the **ping** command from the host to ping an IP address on the network segment specified by free IP.

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The output shows that you can access that segment before passing 802.1X authentication. If you use a Web browser to access any external website except the free IP segments, you are redirected to the Web server, which provides the 802.1X client software download service. Enter the external website address in dotted decimal notation (for example, 3.3.3.3 or http://3.3.3.3) in the address bar.

Configuration files

```
#
 domain default enable test
#
 dhcp relay server-group 1 ip 192.168.2.2
#
 dot1x
 dot1x url http://192.168.2.3
 dot1x free-ip 192.168.2.0 255.255.255.0
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
```

```
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface Vlan-interface2
 ip address 192.168.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
```

AAA configuration examples

AAA manages users in the same ISP domain based on their access types. The device supports the following user access types:

- **LAN**—LAN users must pass 802.1X or MAC authentication to get online.
- **Login**—Login users include SSH, Telnet, FTP, and terminal users who log in to the device.
- **Portal**—Portal users must pass portal authentication to access the network.

This chapter provides authentication and authorization configuration examples for the user access types in different network scenarios.

Example: Configuring local authentication and authorization for FTP users

Applicable product matrix

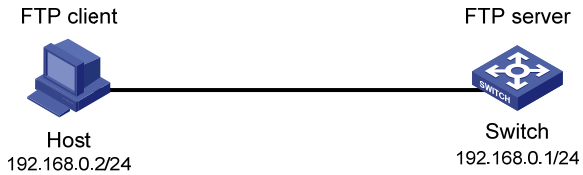
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 21, users on the host can access the switch through FTP.

Configure the switch to implement local authentication and authorization for FTP users.

Figure 21 Network diagram



Configuration restrictions and guidelines

When you configure local authentication and authorization, follow these restrictions and guidelines:

- By default, the switch uses the default ISP domain named **system**.
- When you configure the default ISP domain, make sure the specified domain exists. All users whose usernames do not include domain names are authenticated in the default ISP domain.
- The switch selects the ISP domain for user authentication in the following order:

- ISP domain specified for authentication by the access module such as 802.1X, portal, and MAC authentication.
- ISP domain included in the username.
- Default ISP domain.

Configuration procedures

Configure the IP address of VLAN-interface 1 as 192.168.0.1, through which FTP users access the switch.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch–Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Switch-Vlan-interface1] quit
```

Enable the FTP server function.

```
[Switch] ftp server enable
```

Create a local user account named **ftp**.

```
[Switch] local-user ftp
New local user added.
```

Configure the password to **pwd** in plain text for the local user **ftp**.

```
[Switch-luser-ftp] password simple pwd
```

Configure the FTP service type for the local user **ftp**.

```
[Switch-luser-ftp] service-type ftp
[Switch-luser-ftp] quit
```

Configure the switch to implement local authentication and authorization for login users in the ISP domain named **system**.

```
[Switch] domain system
[Switch-isp-system] authentication login local
[Switch-isp-system] authorization login local
[Switch-isp-system] quit
```

Verifying the configuration

Access the switch through FTP by using username **ftp@system** and password **pwd**. The FTP connection is successfully established between the host and the switch.

```
c:\> ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User(192.168.0.1:(none)):ftp@system
331 Password required for ftp@system.
Password:
230 User logged in.
ftp>
```

Configuration file

```
#
 ftp server enable
#
 domain default enable system
#
domain system
 authentication login local
 authorization login local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user ftp
 password cipher $c$3$05fBix1tIUftQUq3Ya+xWoF9J6dBSg==
 service-type ftp
#
interface Vlan-interface1
 ip address 192.168.0.1 255.255.255.0
#
```

Example: Configuring RADIUS authentication and authorization for Telnet users

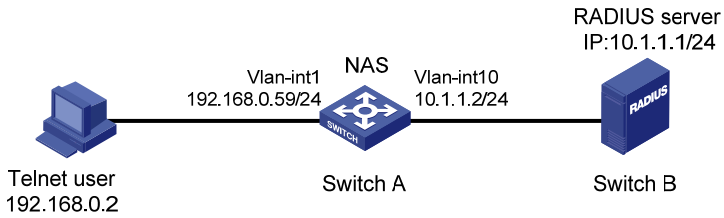
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 22, configure Switch A to implement RADIUS authentication and authorization for Telnet users.

Figure 22 Network diagram



Configuration restrictions and guidelines

When you configure RADIUS authentication and authorization for Telnet users, follow these restrictions and guidelines:

- The authentication mode of user interfaces is set by the **authentication-mode** command and affects access to commands for login users.
  - In AAA (**scheme**) mode, the authorized command level determines the commands available for each login user.
  - In password (**password**) or no authentication (**none**) mode, access to commands is determined by the user interface.
- The standard RADIUS authentication port is 1812. This example uses an HP 5500 HI series switch as the RADIUS server and uses UDP port 1645 for RADIUS authentication.

Configuration procedures

Configuring interfaces

Configure the IP addresses for interfaces as shown in Figure 22, and make sure the host, server, and switches can reach each other.

Configuring Switch A

Enable the Telnet server function.

```
<SwitchA> system-view
[SwitchA] telnet server enable
```

Configure the switch to use AAA for Telnet users.

```
[SwitchA] user-interface vty 0 15
[SwitchA-ui-vty0-15] authentication-mode scheme
[SwitchA-ui-vty0-15] quit
```

Create a RADIUS scheme named **rad**.

```
[SwitchA] radius scheme rad
New Radius scheme
```

Configure the primary RADIUS authentication server, whose IP address is 10.1.1.1, authentication port is 1645, and shared key is **abc**.

```
[SwitchA-radius-rad] primary authentication 10.1.1.1 1645 key abc
```

Configure the switch to remove the domain names from usernames to be sent to the RADIUS server.

```
[SwitchA-radius-rad] user-name-format without-domain
```

Specify the source IP address for outgoing RADIUS packets as 10.1.1.2.

```
[SwitchA-radius-rad] nas-ip 10.1.1.2
```

Set the RADIUS server type to **standard**.

```
[SwitchA-radius-rad] server-type standard
[SwitchA-radius-rad] quit
```

Create an ISP domain named **domain1**.

```
[SwitchA] domain domain1
```

Configure the switch to use RADIUS scheme **rad** as the authentication method for login users in the ISP domain. Use local authentication as the backup authentication method.

```
[SwitchA-isp-domain1] authentication login radius-scheme rad local
```

Configure the switch to use RADIUS scheme **rad** as the authorization method for login users in the ISP domain. Use local authentication as the backup authorization method.

```
[SwitchA-isp-domain1] authorization login radius-scheme rad local
```

Configure the accounting method for login users as **none**.

```
[SwitchA-isp-bbb] accounting login none
[SwitchA-isp-domain1] quit
```

Configure **domain1** as the system default ISP domain.

```
[SwitchA] domain default enable domain1
```

Create a local user named **telnet1** and configure the Telnet service type and plaintext password **123456** for the user.

```
[SwitchA] local-user telnet1
[SwitchA-luser-telnet1] service-type telnet
[SwitchA-luser-telnet1] password simple 123456
[SwitchA-luser-telnet1] quit
```

Configuring Switch B

Create a local user named **telnet1**.

```
<SwitchB> system-view
[SwitchB] radius-server user telnet1
```

Set the user's password to **123456** in plain text.

```
[SwitchB-rdsuser-telnet1] password simple 123456
[SwitchB-rdsuser-telnet1] quit
```

Configure the IP address of the RADIUS client as 10.1.1.2 and the shared key is **abc** in plain text.

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

Verifying the configuration

Telnet to Switch A by entering the username **telnet1@domain1** or **telnet1** and password **123456**. You will pass authentication and can log in to the user interface on Switch A.

```
******************************************************************************
* Copyright (c) 2004-2013 Hewlett-Packard Development Company,L.P.           *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

```
Login authentication


Username:telnet1@domain1
Password:
<SwitchA>
```

Display connection information on Switch A to see the Telnet user information.

```
<SwitchA> display connection
Slot:  1
Index=1   ,Username=telnet1@domain1
IP=192.168.0.2
IPv6=N/A

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

Configuration files

- Switch A:

```
#
 telnet server enable
#
radius scheme rad
 primary authentication 10.1.1.1 1645 key cipher
$c$3$A5ng5y1DclDYJiLkhovxImB09cAe3w==
 user-name-format without-domain
 nas-ip 10.1.1.2
#
domain domain1
 authentication login radius-scheme rad local
 authorization login radius-scheme rad local
 accounting login none
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user telnet1
 password cipher $c$3$albKG13b86oIx1t+U1YIbKe9R4fJufa35Q==
 service-type telnet
#
user-interface vty 0 15
 authentication-mode scheme
#
```

- Switch B:

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$EEKWoSNy6Om3tZ0PhUbTPLuWMY2+aw==
#
```

```
radius-server user telnet1
 password cipher $c$3$4rJuGA/vjrZHO+o33+/NPkcVZWuY8nnDzw==
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
```

Example: Configuring RADIUS authentication and authorization for SSH users

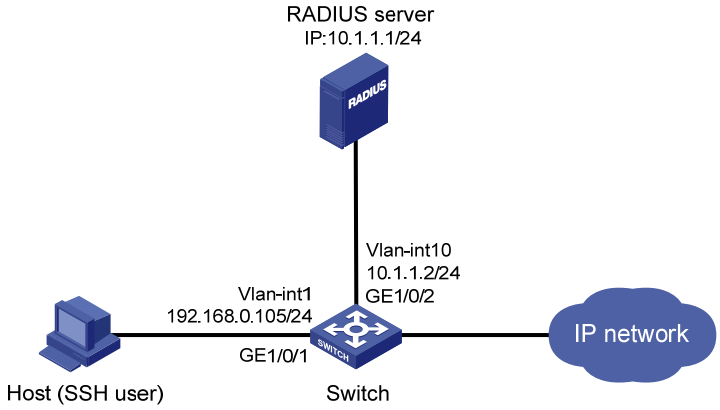
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 23, configure the switch to implement RADIUS authentication and authorization for SSH users.

Figure 23 Network diagram



Requirements analysis

1. To implement remote RADIUS authentication and authorization, complete the following tasks on the RADIUS server that runs on IMC:
   - Add the switch to IMC as an access device for management.
   - Create a device management user account for the SSH user, including the account name, password, service type, and command level.

2. To communicate with the RADIUS server and host, you must enable the RADIUS client and SSH server functions on the switch.

Configuration restrictions and guidelines

The RADIUS server in this example runs on IMC PLAT 5.2 (E0401) and IMC UAM 5.2 (E0402). The configuration examples vary with IMC versions, deployed service components, and UAM system settings. For more information, see *HP IMC User Access Manager Administrator Guide*.

Configuration procedures

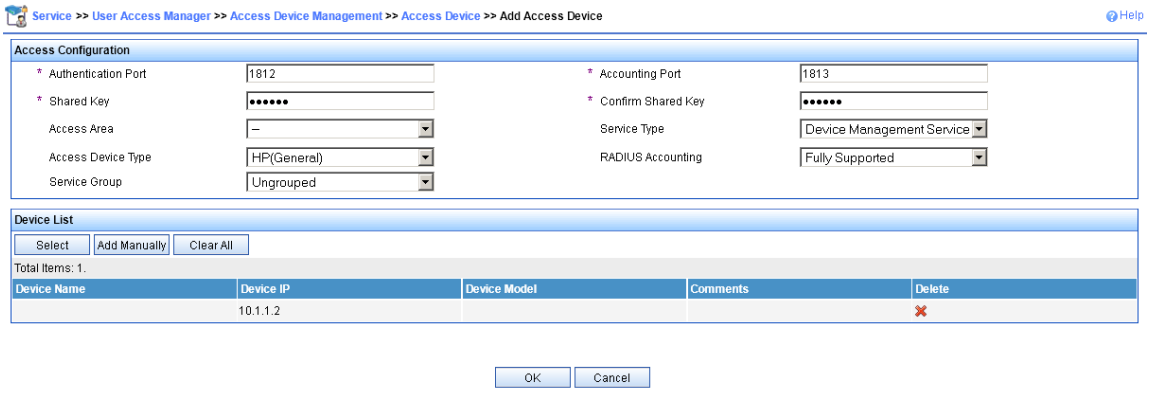
Configuring interfaces

Configure the IP addresses for interfaces as shown in Figure 23, and make sure the host, server, and switch can reach each other.

Configuring the RADIUS server

1. Add the switch to IMC as an access device:
   a. Click the **Service** tab and select **User Access Manager** > **Access Device Management** > **Access Device** from the navigation tree.
   b. Click **Add**.
   c. In the **Access Configuration** area, configure the following parameters:
      – Enter **1812** in the **Authentication Port** field.
      – Enter **1813** in the **Accounting Port** field.
      – Enter **aabbcc** in **Shared Key** and **Confirm Shared Key** fields.
      – Select **Device Management Service** from the **Service Type** list.
      – Select **HP(General)** from the **Access Device Type** list.
   d. On the **Device List**, click **Select** or **Add Manually** to specify 10.1.1.2 as the device IP address.
   e. Click **OK**.

Figure 24 Adding an access device in IMC



2. Create a device management user account for the SSH user:

a. Click the **User** tab and select **User Access Manager** > **Access User View** > **Device Mgmt User** from the navigation tree.

b. Click **Add**.

c. In the **Basic Information of Device Management User** area, configure the following parameters:

   – Enter **hello@bbb** in the **Account Name** field.

   – Enter **123456** in **User Password** and **Confirm Password** fields.

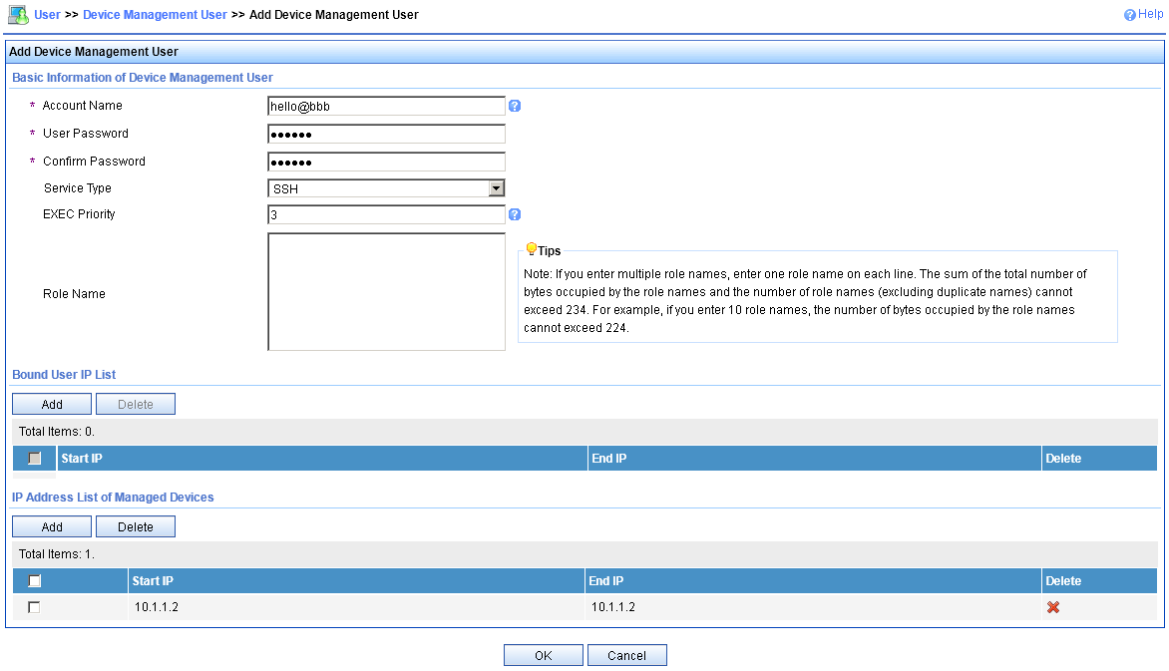
   – Select **SSH** from the **Service Type** list.

   – Select **3** from the **EXEC Priority** list.

d. In the **IP Address List of Managed Devices** area, click **Add** to specify 10.1.1.2 as the start and end IP addresses.

e. Click **OK**.

Figure 25 Adding a device management user account in IMC



Configuring the switch

Configure the IP address of VLAN-interface 1, through which the user connects to the SSH server.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch–Vlan-interface1] ip address 192.168.0.105 255.255.255.0
[Switch-Vlan-interface1] quit
```

Configure the IP address of VLAN-interface 10, through which the switch communicates with the RADIUS server.

```
[Switch] vlan 10
[Switch-vlan10] port gigabitethernet1/0/2
[Switch-vlan10] quit
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface10] quit
```

Create local RSA and DSA key pairs and enable the SSH server.

```
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
+++.+++++++++++++
++++++++
++++
+++++++

[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
++++++++++++
[Switch] ssh server enable
Info: Enable SSH server.
```

Configure the switch to use AAA for SSH users.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
```

Create a RADIUS scheme named **rad**.

```
[Switch] radius scheme rad
New Radius scheme
```

Configure the primary authentication server with IP address 10.1.1.1 and authentication port number 1812.

```
[Switch-radius-rad] primary authentication 10.1.1.1 1812
```

Set the shared key for secure RADIUS authentication communication to **aabbcc**.

```
[Switch-radius-rad] key authentication aabbcc
```

Configure the switch to include the domain name in usernames to be sent to the RADIUS server.

```
[Switch-radius-rad] user-name-format with-domain
```

Configure the RADIUS server type, which must be **extended** for IMC.

```
[Switch-radius-rad] server-type extended
[Switch-radius-rad] quit
```

Configure the authentication and authorization methods for login users in ISP domain **bbb**.

```
[Switch] domain bbb
```

```
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit
```

Configuring the host

Configure the SSH client on the host. The configuration procedure varies with SSH client software. For more information, see *SSH Configuration Examples*.

Verifying the configuration

Access the switch through SSH by using username **hello@bbb** and password **123456**. After login, the user can use the commands of levels 0 through 3.

Use the **display connection** command to view user connection information on the switch.

```
[Switch] display connection
Slot:  1
Index=1 , Username=hello@bbb
 IP=192.168.0.58
 IPv6=N/A

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

Configuration file

```
#
vlan 10
#
radius scheme rad
 server-type extended
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface Vlan-interface1
 ip address 192.168.0.105 255.255.255.0
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port access vlan 10
#
ssh server enable
#
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#
```

Example: Configuring RADIUS authentication and authorization for different user types

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

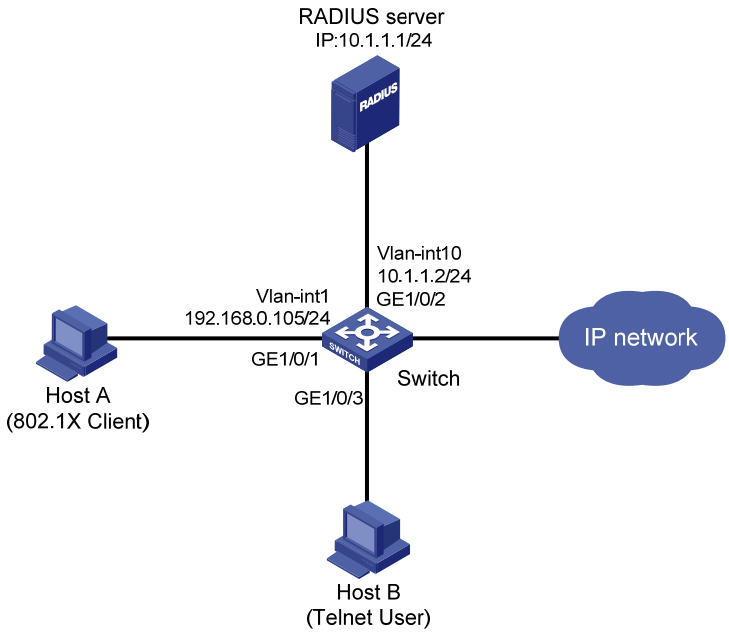
Network requirements

As shown in Figure 26, the RADIUS server runs on IMC to provide authentication and authorization.

Configure the switch to complete the following functions:

- Uses the RADIUS server for authentication and authorization of 802.1X users from Host A.
- Implements local authentication and authorization for Telnet users from Host B.

Figure 26 Network diagram



Configuration restrictions and guidelines

The RADIUS server in this example runs on IMC PLAT 5.2 (E0401) and IMC UAM 5.2 (E0402). The configuration examples vary with IMC versions, deployed service components, and UAM system settings. For more information, see *HP IMC User Access Manager Administrator Guide*.

Configuration procedures

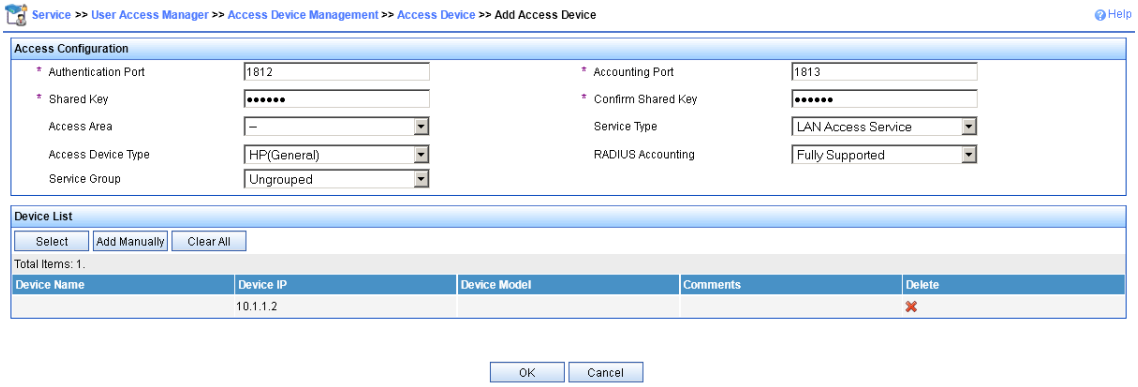
Configuring interfaces

Configure the IP addresses for interfaces as shown in Figure 26. Make sure the hosts, server, and switch can reach each other.

Configuring the RADIUS server

1. Add the switch to IMC as an access device:
   a. Click the **Service** tab and select **User Access Manager** > **Access Device Management** > **Access Device** from the navigation tree.
   b. Click **Add**.
   c. In the **Access Configuration** area, configure the following parameters:
      – Enter **1812** in the **Authentication Port** field.
      – Enter **1813** in the **Accounting Port** field.
      – Enter **aabbcc** in **Shared Key** and **Confirm Shared Key** fields.
      – Select **LAN Access Service** from the **Service Type** list.
      – Select **HP(General)** from the **Access Device Type** list.
   d. On the **Device List**, click **Select** or **Add Manually** to specify 10.1.1.2 as the device IP address.
   e. Click **OK**.

Figure 27 Adding an access device in IMC

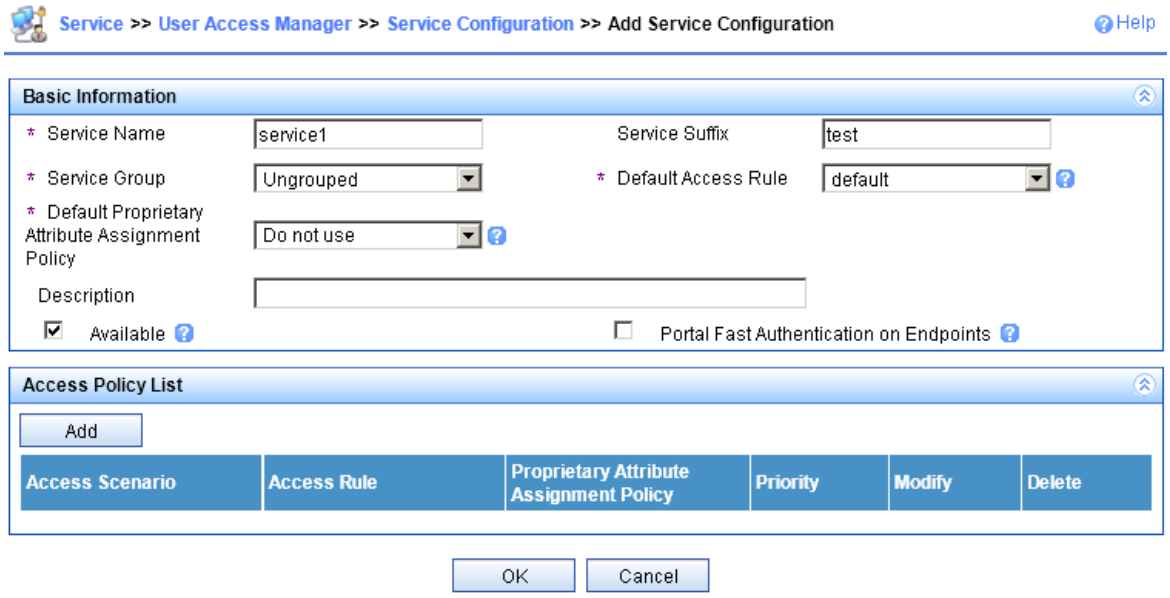


2. Create an access rule:
   a. From the navigation tree, select **User Access Manager** > **Access Rule Management**.
   b. Click **Add**.
   c. Enter **default** in the **Access Rule Name** field and use the default settings of other parameters.
   d. Click **OK**.

Figure 28 Adding an access rule in IMC

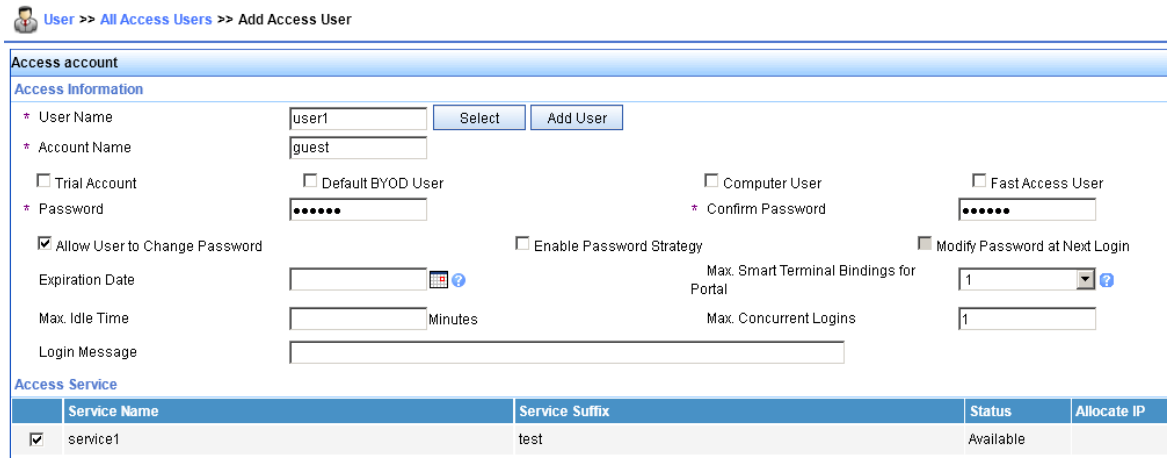
3. Create a service:
   a. From the navigation tree, select **User Access Manager** > **Service Configuration**.
   b. Click **Add**.
   c. In the **Basic Information** area, configure the following parameters:
      – Enter **service1** in the **Service Name** field.
      – Enter **test** in the **Service Suffix** field.
      – Select **default** from the **Default Access Rule** list.
      – Use the default settings of other parameters.
   d. Click **OK**.

Figure 29 Adding a service in IMC



4. Create an access user account and assign the service to the account:
   a. Click the **User** tab and select **User Access Manager** > **Access User View** > **All Access Users** from the navigation tree.
   b. Click **Add**.
   c. In the **Access Information** area, configure the following parameters:
      – Click **Add User** to create a Platform user named **user1**.
      – Enter **guest** in the **Account Name** field to identify the 802.1X user.
      – Enter **123456** in **Password** and **Confirm Password** fields.
      – Use the default settings of other parameters.
   d. In the **Access Service** area, select **service1** on the list.
   e. Click **OK**.

Figure 30 Adding an access user account in IMC



Configuring the switch

Enable the Telnet server function.

```
<Switch> system-view
[Switch] telnet server enable
```

Configure the switch to use AAA for Telnet users.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] protocol inbound telnet
[Switch-ui-vty0-15] quit
```

Configure a local user named **telnet** and set the password to **123456**.

```
[Switch] local-user telnet
New local user added.
[Switch-luser-telnet] service-type telnet
[Switch-luser-telnet] password simple 123456
[Switch-luser-telnet] quit
```

Create a RADIUS scheme named **radius1**.

```
[Switch] radius scheme radius1
[Switch-radius-radius1] primary authentication 10.1.1.1 1812
[Switch-radius-radius1] key authentication aabbcc
[Switch-radius-radius1] server-type extended
[Switch-radius-radius1] quit
```

Create an ISP domain named **test**. Configure the switch to use RADIUS scheme named **radius1** for 802.1X users and to implement local authentication for Telnet users in the ISP domain.

```
[Switch] domain test
[Switch-isp-test] authentication lan-access radius-scheme radius1
[Switch-isp-test] authentication login local
[Switch-isp-test] quit
```

Configure ISP domain **test** as the system default ISP domain.

```
[Switch] domain default enable test
```

Enable 802.1X on interface GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

Configure interface GigabitEthernet 1/0/1 to implement port-based access control. This step is optional because port-based access control is the default setting.

```
[Switch] dot1x port-method macbased interface gigabitethernet 1/0/1
```

Enable 802.1X globally.

```
[Switch] dot1x
```

Verifying the configuration

The user initiates an 802.1X connection on Host A by using an 802.1X client, such as the iNode client. After the user provides the username **guest@test** and password **123456**, the user can access the Internet.

The user on Host B can Telnet to the switch by entering the username **telnet@test** and password **123456**.

Configuration file

```
#
 domain default enable test
#
 telnet server enable
#
 dot1x
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication lan-access radius-scheme radius1
 authentication login local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user telnet
 password cipher $c$3$h9XubfNGPUajFnOqaj8bXlVgB3jlPh+qRA==
 service-type telnet
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound telnet
#
```

Example: Allowing a specific host to access the network

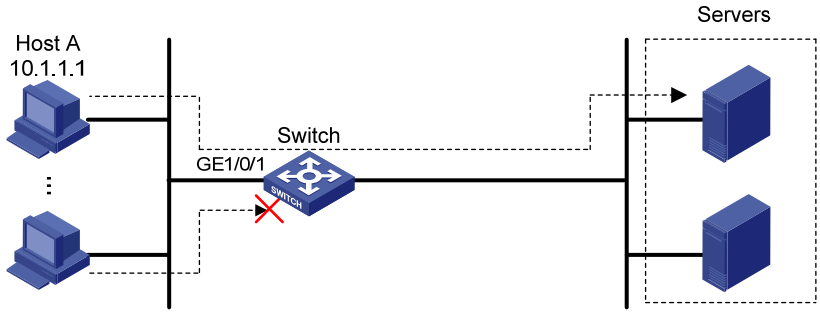
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 31, apply an ACL to GigabitEthernet 1/0/1 to allow packets sourced from Host A only during the period from 8:30 to 18:00 every day.

Figure 31 Network diagram



Requirements analysis

To implement time-based ACL rules, you must configure a time range and apply the time range to the ACL rules.

To filter packets that do not match the permit statement during working hours, you must configure a deny statement after the permit statement.

Configuration restrictions and guidelines

When you configure ACL rules, follow these restrictions and guidelines:

- Use a wildcard mask with an IP address to define a subnet. The wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. For example, to specify subnet 1.1.0.0/16, enter **1.1.0.0 0.0.255.255**.

- ACL rules are order dependent. You must be careful when you add ACL rules. For example, if the deny statement is configured before the permit statement, the interface denies all packets to pass through during the specified time range.

Configuration procedures

Create a periodic time range from 8:30 to 18:00 every day.

```
<Switch> system-view
[Switch] time-range working_time 8:30 to 18:00 daily
```

Configure IPv4 basic ACL 2000 to permit packets sourced from 10.1.1.1 and deny packets sourced from any other addresses during the time range.

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 10.1.1.1 0 time-range working_time
[Switch-acl-basic-2000] rule deny source any time-range working_time
[Switch-acl-basic-2000] quit
```

Apply ACL 2000 to filter incoming IPv4 packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 2000 inbound
```

Verifying the configuration

Display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 2000, Successful
  Out-bound Policy:
```

The output shows that ACL 2000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Verify that the servers can be pinged from Host A during the specified time range, but they cannot be pinged from any other hosts.

Verify that the servers can be pinged from any of the hosts during a period outside of the specified time range.

Configuration files

```
#
 time-range working_time 08:30 to 18:00 daily
#
acl number 2000
 rule 0 permit source 10.1.1.1 0 time-range working_time
 rule 5 deny source any time-range working_time
#
interface GigabitEthernet1/0/1
```

```
 packet-filter 2000 inbound
#
```

Example: Denying a specific host to access the network

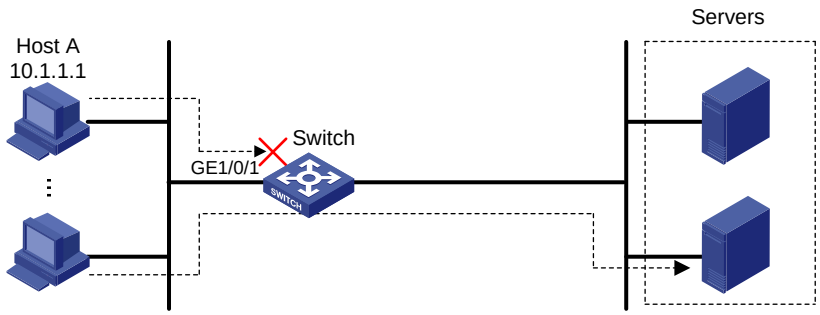
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 32, apply an ACL to GigabitEthernet 1/0/1 to deny packets sourced from Host A only during working hours (from 8:30 to 18:00) every day.

Figure 32 Network diagram



Requirements analysis

To implement time-based ACL rules, you must configure a time range and apply the time range to the ACL rules.

Configuration restrictions and guidelines

When you configure ACL rules, follow these restrictions and guidelines:

- Use a wildcard mask with an IP address to define a subnet. The wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. For example, to specify subnet 1.1.0.0/16, enter **1.1.0.0 0.0.255.255**.
- The packet filtering function permits packets that do not match any ACL rules.

Configuration procedures

Create a periodic time range from 8:30 to 18:00 every day.

```
<Switch> system-view
[Switch] time-range working_time 8:30 to 18:00 daily
```

Create IPv4 basic ACL 2000 and configure a rule to deny packets sourced from 10.1.1.1.

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule deny source 10.1.1.1 0 time-range working_time
[Switch-acl-basic-2000] quit
```

Apply ACL 2000 to filter incoming IPv4 packets on GigabitEthernet1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 2000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 2000, Successful
  Out-bound Policy:
```

The output shows that ACL 2000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Verify that the servers cannot be pinged from Host A during the specified time range, but they can be pinged from any other hosts.

Verify that the servers can be pinged from any of the hosts during a period outside of the specified time range.

Configuration files

```
#
 time-range working_time 08:30 to 18:00 daily
#
acl number 2000
 rule 0 deny source 10.1.1.1 0 time-range working_time
#
interface GigabitEthernet1/0/1
 packet-filter 2000 inbound
#
```

Example: Allowing access between specific subnets

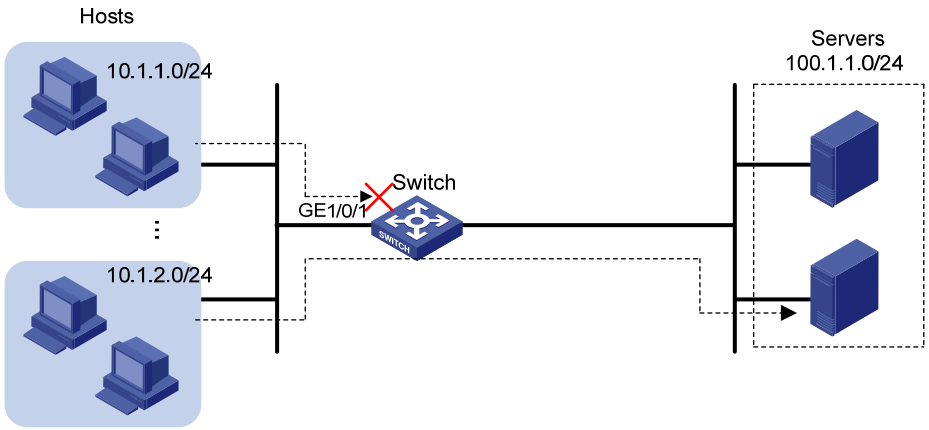
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 33, apply an ACL to allow only packets from 10.1.2.0/24 to 100.1.1.0/24.

Figure 33 Network diagram



Configuration restrictions and guidelines

When you configure ACL rules, follow these restrictions and guidelines:

- Use a wildcard mask with an IP address to define a subnet. The wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. For example, to specify subnet 1.1.0.0/16, enter **1.1.0.0 0.0.255.255**.
- ACL rules are order dependent. You must be careful when you add ACL rules. For example, if the deny statement is configured before the permit statement, the interface denies all packets to pass through.

Configuration procedures

Create IPv4 advanced ACL 3000.

```
<Switch> system-view
[Switch] acl number 3000
```

Add a rule to permit IP packets from 10.1.2.0/24 to 100.1.1.0/24 to pass through.

```
[Switch-acl-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination 100.1.1.0
0.0.0.255
```

Add a rule to deny any IP packets to pass through.

```
[Switch-acl-adv-3000] rule deny ip
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Verify that the servers can be pinged from any of the hosts on subnet 10.1.2.0/24.

Verify that the servers cannot be pinged from any of the hosts on subnet 10.1.1.0/24.

Configuration files

```
#
acl number 3000
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 100.1.1.0 0.0.0.255
 rule 5 deny ip
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
```

Example: Denying Telnet packets

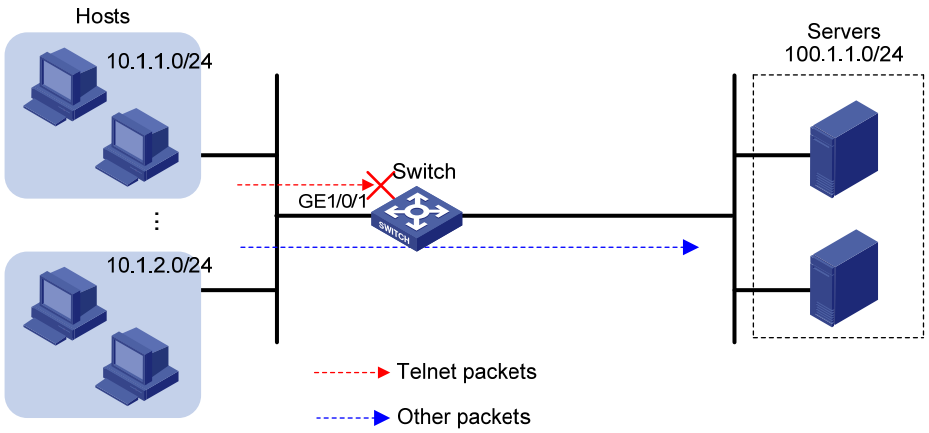
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 34, apply an ACL to GigabitEthernet 1/0/1 so that the interface drops all incoming Telnet packets and allows other IP packets to pass through.

Figure 34 Network diagram



Requirements analysis

To match Telnet packets, you must specify the destination TCP port number 23 in an advanced ACL.

Configuration restrictions and guidelines

The packet filtering function permits packets that do not match any ACL rules.

Configuration procedures

Create IPv4 advanced ACL 3000 and configure a rule to deny packets with destination TCP port 23.

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule 0 deny tcp destination-port eq telnet
```

```
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Ping a server on subnet 100.1.1.0/24 from a host. The server can be pinged successfully. Use the host to Telnet the same server that supports Telnet services. Your Telnet operation fails.

Configuration files

```
#
acl number 3000
 rule 0 deny tcp destination-port eq telnet
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
```

Example: Allowing TCP connections initiated from a specific subnet

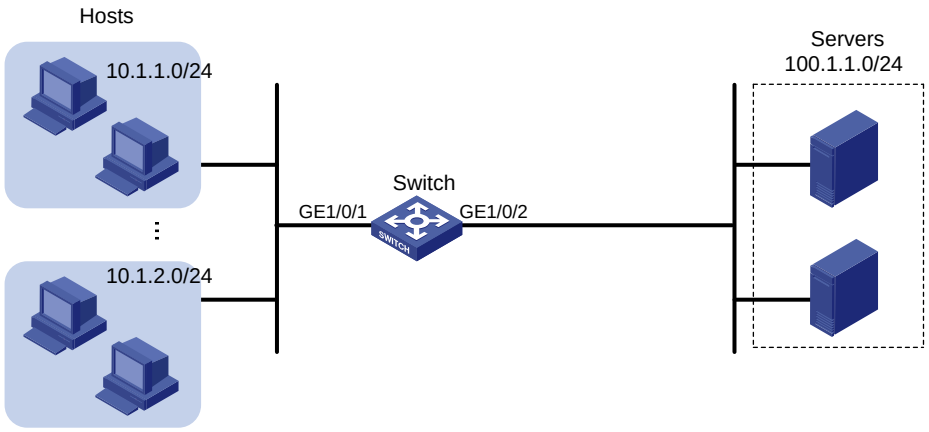
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 35, apply an ACL to allow TCP connections between the hosts and servers except the TCP connections initiated by the servers to hosts in subnet 10.1.1.0/24.

Figure 35 Network diagram



Requirements analysis

To match established TCP connections, you must specify the **established** keyword (the ACK or RST flag bit set) in the advanced ACL rule.

Because a TCP initiator typically uses a TCP port number greater than 1023, you must specify a port number rage greater than 1023 to match connections initiated by the TCP server.

Configuration restrictions and guidelines

When you configure ACL rules, follow these restrictions and guidelines:

- Use the wildcard mask with an IP address to define a subnet. The wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. For example, to specify subnet 1.1.0.0/16, enter **1.1.0.0 0.0.255.255**.
- ACL rules are order dependent. You must be careful when you add ACL rules. For example, if the deny statement is configured before the permit statement, the interface denies all TCP connections initiated by the servers to the hosts in subnet 10.1.1.0/24 to pass through.
- The packet filtering function permits packets that do not match any ACL rules.

Configuration procedures

Create IPv4 advanced ACL 3000.

```
<Switch> system-view
[Switch] acl number 3000
```

Configure a rule to allow TCP packets from the servers to the hosts in subnet 10.1.1.0/24 with TCP port number greater than 1023 and the ACK or RST flag bit set.

```
[Switch-acl-adv-3000] rule permit tcp established source 100.1.1.0 0.0.0.255 destination
10.1.1.0 0.0.0.255 destination-port gt 1023
```

Configure a rule to deny all TCP connection initiated by the servers to the hosts in subnet 10.1.1.0/24.

```
[Switch-acl-adv-3000] rule deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] packet-filter 3000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/2.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/2
Interface: GigabitEthernet1/0/2
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/2 for packet filtering.

Use a host on subnet 10.1.1.0/24 to initiate TCP connections (for example, access a shared folder) to a server on subnet 100.1.1.0/24. The TCP connections can be established.

Use a server on subnet 100.1.1.0/24 to access a shared folder on the host on subnet 10.1.1.0/24. The access is denied.

Verify that hosts on subnet 10.1.2.0/24 and servers can access shared folders of each other.

Configuration files

```
#
acl number 3000
 rule 0 permit tcp established source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
destination-port gt 1023
 rule 5 deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/2
 packet-filter 3000 inbound
#
```

Example: Denying FTP traffic

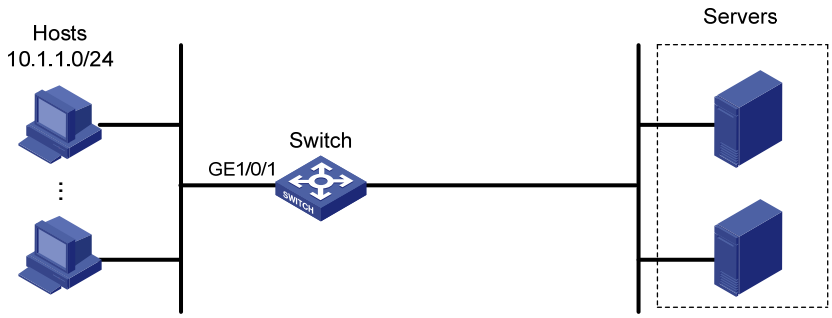
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 36, apply an ACL to GigabitEthernet 1/0/1 to deny FTP traffic destined for the servers.

Figure 36 Network diagram



Requirements analysis

FTP uses TCP port 20 for data transfer and port 21 for FTP control. To identify FTP traffic, you must specify TCP ports 20 and 21 in ACL rules.

Configuration restrictions and guidelines

The packet filtering function permits packets that do not match any ACL rules.

Configuration procedures

Create IPv4 advanced ACL 3000 and a rule in the ACL to deny packets with destination TCP ports 20 and 21.

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny tcp destination-port range 20 21
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Use a host to initiate FTP connection requests to a server that provides FTP services. FTP connection cannot be established.

Configuration files

```
#
acl number 3000
 rule 0 deny tcp destination-port range ftp-data ftp
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
```

Example: Allowing FTP traffic (active FTP)

This example provides an ACL application to allow FTP traffic when FTP operates in active mode. In this mode, the client initiates the control connection, and the server initiates the data connection from the server's port 20 to the client specified random port. If the client is behind the firewall, a connection cannot be established.

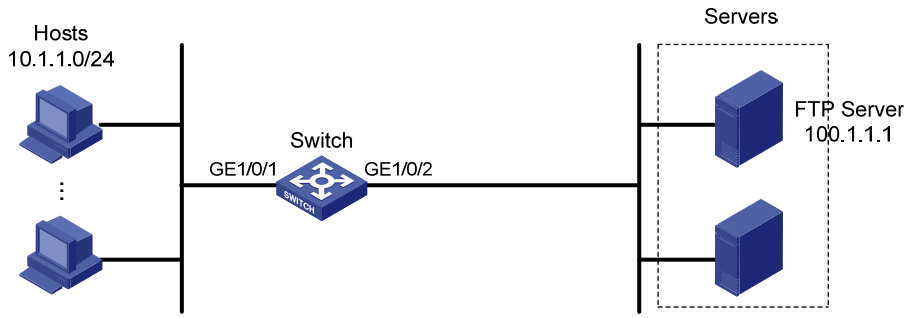
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 37, apply an ACL so that only active FTP traffic is allowed and all other IP traffic is denied.

Figure 37 Network diagram



Requirements analysis

To match FTP control protocol packets, you must specify TCP port 21 in a rule.

To match established FTP data connections, you must specify the **established** keyword and TCP port 20 in a rule.

Configuration procedures

Create IPv4 advanced ACL 3000.

```
<Switch> system-view
[Switch] acl number 3000
```

Configure a rule to permit FTP traffic with destination TCP port 21 and destination IP address 100.1.1.1 from any source IP address.

```
[Switch-acl-adv-3000] rule permit tcp source any destination 100.1.1.1 0 destination-port eq 21
```

Configure a rule to permit established FTP connection traffic with destination TCP port 20 and destination IP address 100.1.1.1 from any source IP address.

```
[Switch-acl-adv-3000] rule permit tcp established source any destination 100.1.1.1 0 destination-port eq 20
```

Configure a rule to deny all IP packets.

```
[Switch-acl-adv-3000] rule deny ip
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming IP packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
[Switch-GigabitEthernet1/0/1] quit
```

Create IPv4 advanced ACL 3001.

```
<Switch> system-view
```

```
[Switch] acl number 3001
```

Configure a rule to permit established FTP connection traffic with source TCP port 20 and source IP address 100.1.1.1.

```
[Switch-acl-adv-3001] rule permit tcp established source 100.1.1.1 0 destination any
source-port eq 20
```

Configure a rule to permit FTP traffic with source TCP port 21 and source IP address 100.1.1.1.

```
[Switch-acl-adv-3001] rule permit tcp source 100.1.1.1 0 destination any source-port eq
21
```

Configure a rule to deny all IP packets.

```
[Switch-acl-adv-3001] rule deny ip
[Switch-acl-adv-3001] quit
```

Apply ACL 3001 to filter incoming IP packets on GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] packet-filter 3001 inbound
```

Verifying the configuration

Use the **display packet-filter all** command to display the application status of incoming and outgoing packet filtering ACLs for all interfaces.

```
[Switch] display packet-filter interface all
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:

  Interface: GigabitEthernet1/0/2
  In-bound Policy:
    acl 3001, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/1 and ACL 3001 has been successfully applied to GigabitEthernet 1/0/2 for packet filtering.

When a server operates in active FTP mode, you can obtain data from the server through FTP.

When a server operates in passive FTP mode, you cannot obtain data from the server through FTP.

Configuration files

```
#
acl number 3000
 rule 0 permit tcp destination 100.1.1.1 0 destination-port eq ftp
 rule 5 permit tcp established destination 100.1.1.1 0 destination-port eq ftp-data
 rule 10 deny ip
acl number 3001
 rule 0 permit tcp established source 100.1.1.1 0 source-port eq ftp-data
 rule 5 permit tcp source 100.1.1.1 0 source-port eq ftp
 rule 10 deny ip
```

```
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
interface GigabitEthernet1/0/2
 packet-filter 3001 inbound
```

Example: Allowing FTP traffic (passive FTP)

This example provides an ACL application to allow FTP traffic when FTP operates in passive mode. In this mode, the FTP client initiates the control connection and data connection to the server. The server uses TCP port 21 for control protocol packets, and uses TCP port greater than 1024 for data packets. When the FTP server denies connections to a port greater than 1024, the passive mode is not applicable.

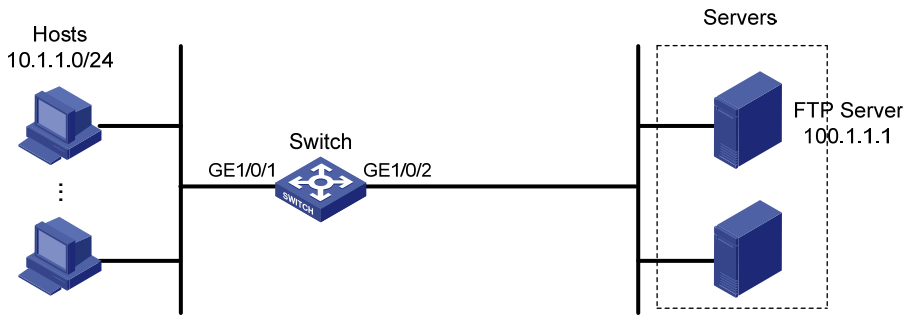
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 38, apply an ACL so that only passive FTP traffic is allowed and all other IP traffic is denied.

Figure 38 Network diagram



Requirements analysis

To match passive FTP traffic, you must specify higher layer protocol matching criteria such as TCP ports. As a result, you must use an advanced ACL. In the ACL, you must configure the correct rules to match the following FTP packets and connections:

FTP packets/connections	Rule settings
FTP protocol control packets destined for the FTP server	Destination TCP port 21.
Established FTP data connections destined for the FTP server	The **established** keyword Destination TCP port greater than 1024
Established FTP protocol control packets destined for the FTP client	Source TCP port 21
Established FTP data connections destined for the FTP client	The **established** keyword Source TCP port greater than 1024

Configuration restrictions and guidelines

When you configure ACL rules, follow these restrictions and guidelines:

- Use the wildcard mask with an IP address to define a subnet. The wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. For example, to specify subnet 1.1.0.0/16, enter **1.1.0.0 0.0.255.255**.
- ACL rules are order dependent. You must be careful when you add ACL rules. For example, if the deny statement is configured before the permit statement, the interface denies all packets to pass through.

Configuration procedures

Create IPv4 advanced ACL 3000.

```
<Switch> system-view
[Switch] acl number 3000
```

Configure a rule to permit packets with destination TCP port 21 and destination IP address 100.1.1.1 from any source IP address.

```
[Switch-acl-adv-3000] rule permit tcp source any destination 100.1.1.1 0 destination-port
eq 21
```

Configure a rule to permit packets with destination IP address 100.1.1.1 and destination TCP port number greater than 1024 from any source IP address.

```
[Switch-acl-adv-3000] rule permit tcp source any destination 100.1.1.1 0 destination-port
gt 1024
```

Configure a rule to deny all IP packets.

```
[Switch-acl-adv-3000] rule deny ip
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming IP packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
[Switch-GigabitEthernet1/0/1] quit
```

Create IPv4 advanced ACL 3001.

```
<Switch> system-view
[Switch] acl number 3001
```

Configure a rule to permit established FTP connection traffic with source TCP port 21 and source IP address 100.1.1.1.

```
[Switch-acl-adv-3001] rule permit tcp established source 100.1.1.1 0 destination any
source-port eq 21
```

Configure a rule to permit established FTP connection traffic with source IP address 100.1.1.1 and source TCP port number greater than 1024.

```
[Switch-acl-adv-3001] rule permit tcp established source 100.1.1.1 0 destination any
source-port gt 1024
```

Configure a rule to deny all IP packets.

```
[Switch-acl-adv-3001] rule deny ip
[Switch-acl-adv-3001] quit
```

Apply ACL 3001 to filter incoming packets on GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] packet-filter 3001 inbound
```

Verifying the configuration

Use the **display packet-filter all** command to display the application status of incoming and outgoing packet filtering ACLs for all interfaces.

```
[Switch] display packet-filter interface all
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:

  Interface: GigabitEthernet1/0/2
  In-bound Policy:
    acl 3001, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/1 and ACL 3001 has been successfully applied to GigabitEthernet 1/0.2 for packet filtering.

When a server operates in passive FTP mode, you can obtain data from the server through FTP.

When a server operates in active FTP mode, you cannot obtain data from the server through FTP.

Configuration files

```
#
acl number 3000
 rule 0 permit tcp destination 100.1.1.1 0 destination-port eq ftp
 rule 5 permit tcp destination 100.1.1.1 0 destination-port gt 1024
 rule 10 deny ip
acl number 3001
 rule 0 permit tcp source 100.1.1.1 0 source-port eq ftp established
 rule 5 permit tcp source 100.1.1.1 0 source-port gt 1024 established
 rule 10 deny ip
```

```
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
interface GigabitEthernet1/0/2
 packet-filter 3001 inbound
```

Example: Allowing ICMP requests from a specific direction

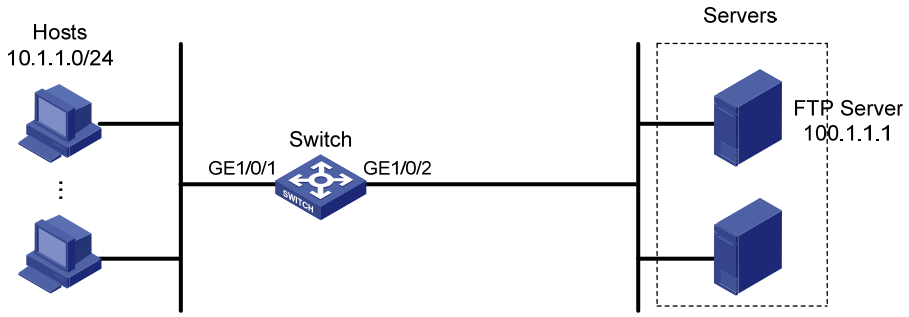
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 39, apply an ACL to deny ICMP requests from the FTP server to the hosts. Only hosts can ping the FTP server.

Figure 39 Network diagram



Requirements analysis

To block ICMP requests from the server to the hosts, you must deny all ICMP echo-request packets on the inbound direction of GigabitEthernet 1/0/2.

Configuration procedures

Create IPv4 advanced ACL 3000, and configure a rule to deny ICMP echo-request packets.

```
<Switch> system-view
```

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny icmp icmp-type echo
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] packet-filter 3000 inbound
[Switch-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/2.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/2
Interface: GigabitEthernet1/0/2
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/2 for packet filtering.

Ping the FTP server from a host. The FTP server can be pinged successfully.

Ping the host from the FTP server. The host cannot be pinged.

Configuration files

```
#
acl number 3000
 rule 0 deny icmp icmp-type echo
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
```

Example: Allowing HTTP/Email/DNS traffic

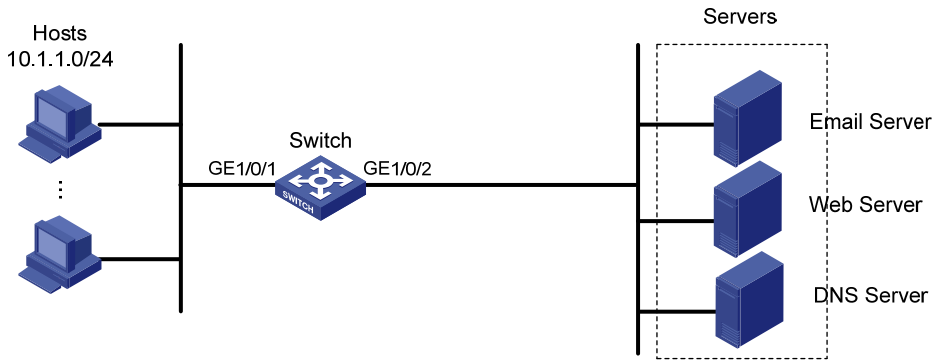
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 40, apply an ACL to GigabitEthernet 1/0/1 to allow only Email, HTTP, and DNS traffic from the server to the hosts. The rest of the traffic sourced from the servers to the hosts is denied.

Figure 40 Network diagram



Configuration restrictions and guidelines

ACL rules are order dependent. You must be careful when you add ACL rules. For example, if the deny statement is configured before the permit statements, the interface denies all packets to pass through.

Configuration procedures

Create IPv4 advanced ACL 3000.

```
<Switch> system-view
[Switch] acl number 3000
```

Add rules to permit only packets with the following destination TCP ports: 25 (SMTP), 110 (POP3), 80 (HTTP), and 53 (DNS).

```
[Switch-acl-adv-3000] rule permit tcp destination-port eq 25
[Switch-acl-adv-3000] rule permit tcp destination-port eq 110
[Switch-acl-adv-3000] rule permit tcp destination-port eq 80
[Switch-acl-adv-3000] rule permit tcp destination-port eq 53
[Switch-acl-adv-3000] rule deny ip
[Switch-acl-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
[Switch-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
```

The output shows that ACL 3000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Ping a server from a host. The server cannot be pinged.

The host can obtain HTTP services from the HTTP server, Email service from the Email server, and DNS service from the DNS server.

Configuration files

```
#
acl number 3000
 rule 0 permit tcp destination-port eq smtp
 rule 5 permit tcp destination-port eq pop3
 rule 10 permit tcp destination-port eq www
 rule 15 permit tcp destination-port eq domain
 rule 20 deny ip
#
interface GigabitEthernet1/0/1
 packet-filter 3000 inbound
```

Example: Filtering packets by MAC address

Ethernet frame header ACLs, also called "Layer 2 ACLs," match packets based on Layer 2 protocol header fields, such as source MAC address and link layer protocol type.

Ethernet frame header ACLs are numbered in the range of 4000 to 4999.

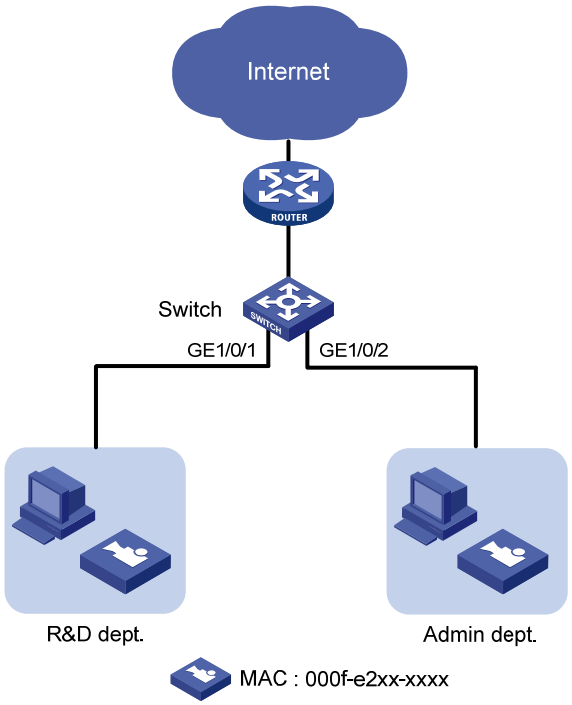
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 41, apply an ACL to permit traffic sourced from video devices in the intranet only during working hours (from 8:30 to 18:00) every day.

Figure 41 Network diagram



Requirements analysis

To match packets from or to a device whose IP address might change, you must use Later 2 ACLs.

To specify devices with the same MAC address prefix, you must use the MAC address mask.

Configuration procedures

Create two periodic time ranges. Time range **time1** is from 00 to 8:30 every day, and time range **time2** is from 18:00 to 24:00 every day.

```
<Switch> system-view
[Switch] time-range time1 0:00 to 8:30 daily
[Switch] time-range time1 18:00 to 24:00 daily
```

Create Ethernet frame header ACL 4000 and configure two rules to deny packets with the source MAC address prefix 000f-e2 in time ranges **time1** and **time2**.

```
[Switch] acl number 4000
[Switch-acl-ethernetframe-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000
time-range time1
[Switch-acl-ethernetframe-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000
time-range time2
[Switch-acl-ethernetframe-4000] quit
```

Apply ACL 4000 to filter incoming packets on GigabitEthernet 1/0/1.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 4000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display the application status of incoming and outgoing packet filtering ACLs for GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 4000, Successful
  Out-bound Policy:
```

The output shows that ACL 4000 has been successfully applied to GigabitEthernet 1/0/1 for packet filtering.

Video devices can communicate with devices in the external network only during the working hours.

Configuration files

```
#
 time-range time1 00:00 to 08:30 daily
 time-range time1 18:00 to 24:00 daily
#
acl number 4000
 rule 0 deny source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1
 rule 5 deny source-mac 000f-e200-0000 ffff-ff00-0000 time-range time2
#
interface GigabitEthernet1/0/1
 packet-filter 4000 inbound
```

Example: Applying ACLs in device management

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

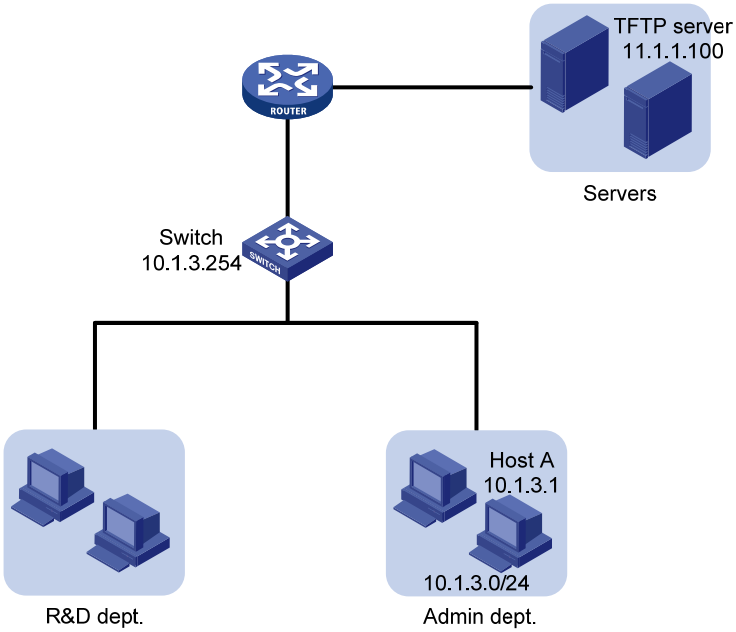
Network requirements

As shown in Figure 42, configure an ACL to implement the following:

- Host A can Telnet to the switch during working hours (from 8:30 to 18:00) on working days.

- The switch can only obtain files from the TFTP server at 11.1.1.100.
- Only Host A can access the switch when the switch functions as the FTP server.

Figure 42 Network diagram



Requirements analysis

To control Telnet, FTP, or TFTP access, you must apply an ACL as follows:

- To control Telnet access, apply the ACL to VTY user interfaces.
- To control FTP or TFTP access, use the **ftp server acl** or **tftp-server acl** command, respectively.

In the ACL, you only need to configure permit rules. The application denies all traffic that does not match the permit rules.

Configuration restrictions and guidelines

When you configure ACL rules, follow these restrictions and guidelines:

- Use the wildcard mask with an IP address to define a subnet. The wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. For example, to specify subnet 1.1.0.0/16, enter **1.1.0.0 0.0.255.255**.
- If a packet does not match any rule in the ACL, the default action is **deny**, and the switch always drops the packet. Therefore, you do not need to configure a deny statement at the end of each ACL.

Configuration procedures

- Control Telnet access to the switch:

  # Define a periodic time range from 08:30 to 18:00 on working days.

  ```
  <Switch> system-view
  ```

```
[Switch] time-range telnet 8:30 to 18:00 working-day
```

Create IPv4 basic ACL 2000 and configure a rule to allow IP packets only sourced from Host A during the time range.

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 10.1.3.1 0 time-range telnet
[Switch-acl-basic-2000] quit
```

Apply ACL 2000 to all VTY user interfaces to allow only Host A to Telnet to the switch.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] acl 2000 inbound
```

- Control access to the TFTP server:

  # Create IPv4 basic ACL 2001 and configure a rule to allow IP packets only sourced from the TFTP server.

  ```
  [Switch] acl number 2001
  [Switch-acl-basic-2001] rule permit source 11.1.1.100 0
  [Switch-acl-basic-2001] quit
  ```

  # Apply ACL 2001 to control the access to the TFTP server.

  ```
  [Switch] tftp-server acl 2001
  ```

- Control access to the FTP server:

  # Create IPv4 basic ACL 2002 and configure a rule to allow IP packets only sourced from Host A.

  ```
  [Switch] acl number 2002
  [Switch-acl-basic-2002] rule permit source 10.1.3.1 0
  [Switch-acl-basic-2002] quit
  ```

  # Enable FTP server on the switch.

  ```
  [Switch] ftp server enable
  ```

  # Apply ACL 2002 to allow only Host A to access the FTP server.

  ```
  [Switch] ftp server acl 2002
  ```

Verifying the configuration

Verify the configuration according to the network requirements. If the requirements are met, the ACL configuration succeeds.

Configuration files

```
#
 ftp server enable
 ftp server acl 2002
#
 time-range telnet 08:30 to 18:00 working-day
#
acl number 2000
 rule 0 permit source 10.1.3.1 0 time-range telnet
acl number 2001
 rule 0 permit source 11.1.1.100 0
acl number 2002
```

```
 rule 0 permit source 10.1.3.1 0
#
 tftp-server acl 2001
#
user-interface vty 0 4
 acl 2000 inbound
```

ARP attack protection configuration examples

This chapter provides ARP attack protection configuration examples.

For more information about ARP attack protection, see *ARP Attack Protection Technology White Paper*.

Example: Configuring ARP source suppression and ARP black hole routing

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

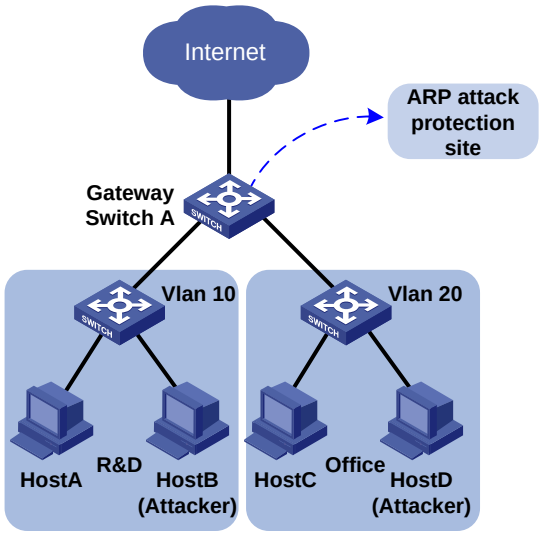
Network requirements

As shown in Figure 43, Host B sends a large number of unresolvable IP packets with the same source address, and Host D sends a large number of unresolvable IP packets with different source addresses.

Configure ARP source suppression and ARP black hole routing on Switch A to meet the following requirements:

- The packets from Host A and Host C can be forwarded correctly.
- The packets from Host B and Host D are discarded.

Figure 43 Network diagram



Configuration procedures

1. Configuring ARP source suppression:

   # Enable ARP source suppression on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] arp source-suppression enable
   ```

   # Set the maximum number of unresolvable packets that can be received from a host in 5 seconds to 100. If the number of unresolvable IP packets received from a host within 5 seconds exceeds 100, Switch A stops resolving packets from the host until the 5 seconds elapse.

   [SwitchA] arp source-suppression limit 100

2. Enable ARP black hole routing on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] arp resolving-route enable
   ```

Verifying the configuration

Display ARP source suppression configuration on Switch A.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
 Current cache length: 16
```

Table 2 Command output

Field	Description
Current suppression limit	Maximum number of unresolvable IP packets that can be received from the same source address within 5 seconds.
Current cache length	Cache size for recording the ARP source suppression information.

Configuration files

```
#
 arp source-suppression enable
 arp source-suppression limit 100
#
```

Example: Configuring source MAC-based ARP attack detection

Applicable product matrix

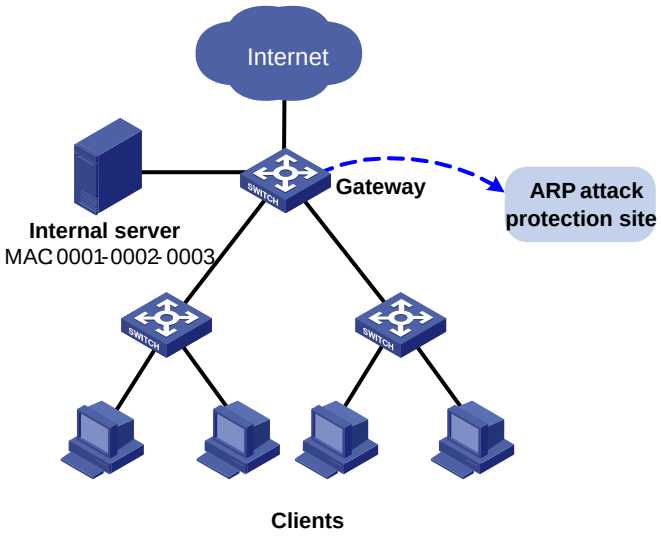
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 44, configure source MAC-based ARP attack detection on the gateway to meet the following requirements:

- If the number of ARP packets received from the same MAC address within 5 seconds exceeds a specific threshold, the gateway adds the MAC address in an ARP attack entry.
- Before the ARP attack entry is aged out, the gateway generates log messages and filters out subsequent ARP packets from that MAC address.
- ARP packets from the internal server with MAC address 0001-0002-0003 are not inspected.

Figure 44 Network diagram



Configuration procedures

Enable source MAC-based ARP attack detection and specify the handling method as **filter**.

```
<Gateway> system-view
[Gateway] arp anti-attack source-mac filter
```

Set the threshold to 30 for source MAC-based ARP attack detection.

```
[Gateway] arp anti-attack source-mac threshold 30
```

Set the aging timer to 60 seconds for ARP attack detection entries.

```
[Gateway] arp anti-attack source-mac aging-time 60
```

Exclude MAC address 0001-0002-0003 from source MAC-based ARP attack detection.

```
[Gateway] arp anti-attack source-mac exclude-mac 0001-0002-0003
```

Verifying the configuration

Display source MAC-based ARP attack detection entries.

```
<Sysname> display arp anti-attack source-mac slot 2
Source-MAC          VLAN ID          Interface            Aging-time
23f3-1122-3344      4094             GE2/0/1              10
23f3-1122-3355      4094             GE2/0/2              30
23f3-1122-33ff      4094             GE2/0/3              25
23f3-1122-33ad      4094             GE2/0/4              30
23f3-1122-33ce      4094             GE2/0/5              2
```

Configuration files

```
#
 arp anti-attack source-mac filter
 arp anti-attack source-mac exclude-mac 0001-0002-0003
 arp anti-attack source-mac aging-time 60
 arp anti-attack source-mac threshold 30
#
```

Example: Configuring ARP detection (by using DHCP snooping entries)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

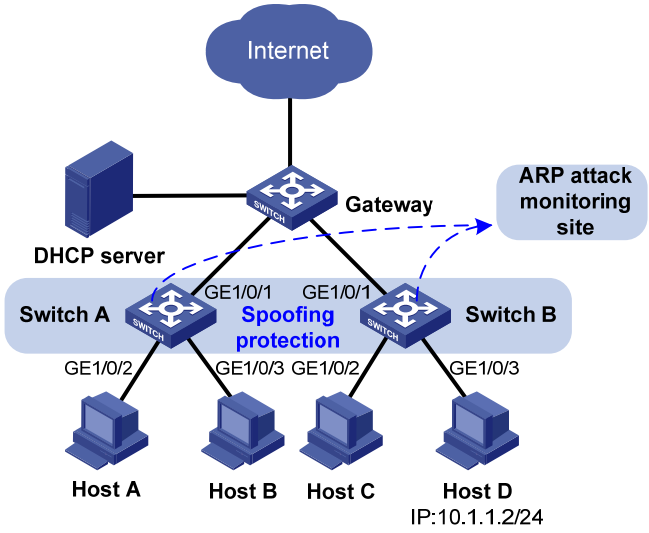
Network requirements

As shown in Figure 45:

- Host A, Host B, Host C, and Host D are in VLAN 1.
- Host A, Host B, and Host C obtain IP addresses from the DHCP server.
- Host D has a manually configured IP address.

Configure ARP detection by using DHCP snooping entries on Switch A and Switch B. This feature enables the switches to forward ARP packets from Host A, Host B, and Host C, and discard the packets from Host D.

Figure 45 Network diagram



Requirements analysis

To prevent user and gateway spoofing, enable ARP detection on Switch A and Switch B to perform ARP packet validity check and user validity check.

To implement ARP detection by using DHCP snooping entries, configure DHCP snooping on Switch A and Switch B.

Configuration restrictions and guidelines

If both ARP packet validity check and user validity check are enabled, the switch performs packet validity check first, and then the user validity check.

Configuration procedures

1. Configure Switch A:

   # Configure DHCP snooping.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/1] quit
```

   # Enable ARP detection for VLAN 1 for user validity check.

```
[SwitchA] vlan 1
[SwitchA-vlan1] arp detection enable
[SwitchA-vlan1] quit
```

Configure the upstream interface as an ARP trusted interface. (By default, an interface is an ARP untrusted interface.)

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] arp detection trust
[SwitchA-GigabitEthernet1/0/1] quit
```

Enable ARP packet validity check.

```
[SwitchA] arp detection validate dst-mac ip src-mac
```

2. Configure Switch B in a similar way as Switch A is configured. (Details not shown.)

Verifying the configuration

If the sender IP and sender MAC of an ARP packet match a DHCP snooping entry, the packet is forwarded. Otherwise, the packet is discarded. You can use the **display dhcp-snooping** command to display DHCP snooping entries.

Configuration files

```
#
 dhcp-snooping
#
vlan 1
 arp detection enable
#
interface GigabitEthernet1/0/1
 dhcp-snooping trust
 arp detection trust
#
 arp detection validate dst-mac ip src-mac
#
```

Example: Configuring ARP detection (by using 802.1X security entries)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

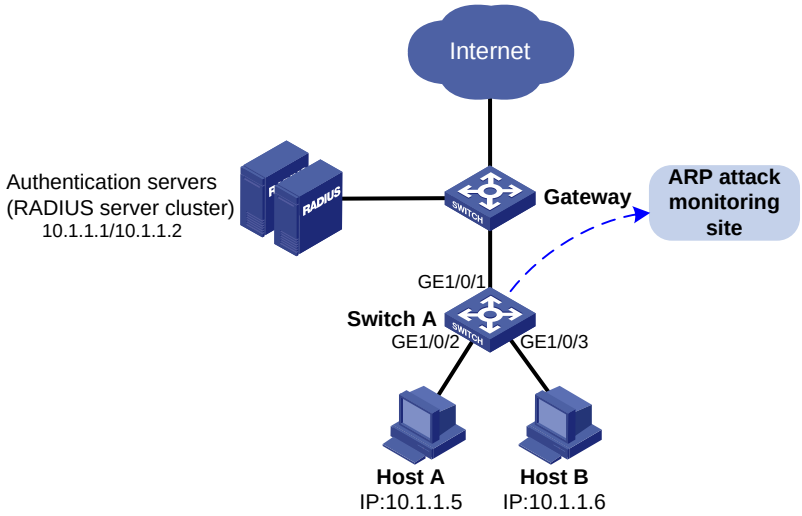
Network requirements

As shown in Figure 46, Host A and Host B use static IP addresses, and they access the gateway and authentication servers through Switch A.

Perform the following tasks for ARP detection:

- Configure the RADIUS server at 10.1.1.1 as the primary authentication server and secondary accounting server.
- Configure the RADIUS server at 10.1.1.2 as the secondary authentication server and primary accounting server.
- Configure ARP detection by using 802.1X security entries on Switch A to forward ARP packets from Host A and Host B when the hosts pass the authentication.

Figure 46 Network diagram



Requirements analysis

To prevent user and gateway spoofing attacks, enable ARP detection for user validity check.

Configuration restrictions and guidelines

802.1X clients must support uploading IP addresses so that the switches can create 802.1X security entries for user validity check.

Configuration procedures

1. Configure the local user account:

   # Add a local user named **localuser**.

   ```
   <SwitchA> system-view
   [SwitchA] local-user localuser
   ```

   # Set the service type to LAN access.

   ```
   [SwitchA-luser-localuser] service-type lan-access
   ```

Set the password to **localpass** in plain text.

```
[SwitchA-luser-localuser] password simple localpass
```

Set the idle timeout period to 20 seconds.

```
[SwitchA-luser-localuser] authorization-attribute idle-cut 20
[SwitchA-luser-localuser] quit
```

2. Configure the RADIUS scheme:

Create a RADIUS scheme named **radius1** and enter its view.

```
[SwitchA] radius scheme radius1
```

Specify the IP address of the primary authentication server as 10.1.1.1 and the IP address of the primary accounting server as 10.1.1.2.

```
[SwitchA-radius-radius1] primary authentication 10.1.1.1
[SwitchA-radius-radius1] primary accounting 10.1.1.2
```

Specify the IP address of the secondary authentication server as 10.1.1.2 and the IP address of the secondary accounting as 10.1.1.1.

```
[SwitchA-radius-radius1] secondary authentication 10.1.1.2
[SwitchA-radius-radius1] secondary accounting 10.1.1.1
```

Set the shared key for secure RADIUS authentication communication to **name**.

```
[SwitchA-radius-radius1] key authentication name
```

Set the shared key for secure RADIUS accounting communication to **money**.

```
[SwitchA-radius-radius1] key accounting money
```

Set the RADIUS server response timeout timer to 5 seconds and the maximum number of RADIUS packet transmission attempts to 5.

```
[SwitchA-radius-radius1] timer response-timeout 5
[SwitchA-radius-radius1] retry 5
```

Set the real-time accounting interval to 15 minutes.

```
[SwitchA-radius-radius1] timer realtime-accounting 15
```

Configure the switch to remove the domain name from the username sent to the RADIUS servers.

```
[SwitchA-radius-radius1] user-name-format without-domain
[SwitchA-radius-radius1] quit
```

3. Configure the ISP domain:

Create domain **aabbcc.net** and enter its view.

```
[SwitchA] domain aabbcc.net
```

Configure the default AAA method for ISP domain **aabbcc.net** to use RADIUS scheme **radius1** and use local method as the backup.

```
[SwitchA-isp-aabbcc.net] authentication default radius-scheme radius1 local
[SwitchA-isp-aabbcc.net] authorization default radius-scheme radius1 local
[SwitchA-isp-aabbcc.net] accounting default radius-scheme radius1 local
```

Set a limit of 30 user connections for ISP domain **aabbcc.net**.

```
[SwitchA-isp-aabbcc.net] access-limit enable 30
```

Specify the idle timeout period for the user as 20 seconds.

```
[SwitchA-isp-aabbcc.net] idle-cut enable 20
[SwitchA-isp-aabbcc.net] quit
```

Configure **aabbcc.net** as the default ISP domain.

```
[SwitchA] domain default enable aabbcc.net
```

4. Configure 802.1X:

Enable 802.1X on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchA] dot1x
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] dot1x
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] dot1x
[SwitchA-GigabitEthernet1/0/3] quit
```

5. Configure ARP detection:

Enable ARP detection for VLAN 1 to check user validity.

```
[SwitchA] vlan 1
[SwitchA-vlan1] arp detection enable
```

Configure the upstream interface as a trusted interface. (An interface is untrusted by default.)

```
[SwitchA-vlan1] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] arp detection trust
[SwitchA-GigabitEthernet1/0/1] quit
```

Verifying the configuration

If the sender IP and sender MAC of an ARP packet from Host A and Host B match an 802.1X security entry, the packet is forwarded. Otherwise, the packet is discarded.

Configuration files

```
#
 domain default enable aabbcc.net
#
 dot1x
#
vlan 1
 arp detection enable
#
radius scheme radius1
 primary authentication 10.1.1.1
 primary accounting 10.1.1.2
 secondary authentication 10.1.1.2
 secondary accounting 10.1.1.1
 key authentication cipher $c$3$DdOHTCT8yNBZxYvle7XkD2Ls5i+A8To=
 key accounting cipher $c$3$2lMkqUQ+POWiHNKtd0a3fwYxlvWvuRp+
 timer realtime-accounting 15
 timer response-timeout 5
 user-name-format without-domain
 retry 5
#
domain aabbcc.net
 authentication default radius-scheme radius1 local
 authorization default radius-scheme radius1 local
```

```
 accounting default radius-scheme radius1 local
 access-limit enable 30
 state active
 idle-cut enable 20 10240
 self-service-url disable
#
local-user localuser
 password cipher $c$3$QF9jpm2ZxRQA8YS5+qedkwIPkWXuIc8FHb+qyQ==
 authorization-attribute idle-cut 20
 service-type lan-access
#
interface GigabitEthernet1/0/1
 arp detection trust
#
interface GigabitEthernet1/0/2
 dot1x
#
interface GigabitEthernet1/0/3
 dot1x
#
```

ARP configuration examples

This chapter provides ARP configuration examples.

Example: Configuring ARP

Applicable product matrix

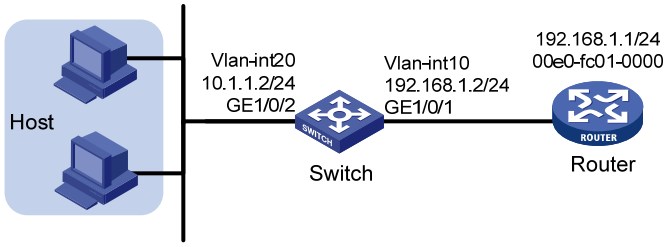
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 47.

- Configure a static ARP entry for the router on the switch to ensure secure communications between the router and switch.
- Set an aging timer for dynamic ARP entries on the switch.

Figure 47 Network diagram



Configuration procedures

Create VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
```

Add interface GigabitEthernet 1/0/1 to VLAN 10.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port access vlan 10
[Switch-GigabitEthernet1/0/1] quit
```

Create VLAN-interface 10 and configure its IP address.

```
[Switch] interface vlan-interface 10
[Switch-vlan-interface10] ip address 192.168.1.2 24
```

```
[Switch-vlan-interface10] quit
```

Create VLAN 20.

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

Add interface GigabitEthernet 1/0/2 to VLAN 20.

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port access vlan 20
[Switch-GigabitEthernet1/0/2] quit
```

Create VLAN-interface 20 and configure its IP address.

```
[Switch] interface vlan-interface 20
[Switch-vlan-interface20] ip address 10.1.1.2 24
[Switch-vlan-interface20] quit
```

Set the aging timer for dynamic ARP entries to 5 minutes.

```
[Switch] arp timer aging 5
```

Configure a static ARP entry. In this entry, the IP address is 192.168.1.1, the MAC address is 00e0-fc01-0000, and the output interface is GigabitEthernet 1/0/1 in VLAN 10.

```
[Switch] arp static 192.168.1.1 00e0-fc01-0000 10 GigabitEthernet 1/0/1
```

Verifying the configuration

Display all ARP entries on the switch.

```
<Switch> display arp
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
192.168.1.1      00e0-fc01-0000  10       GE1/0/1                N/A   S
10.1.1.1         0023-895f-958c  20       GE1/0/2                3     D
10.1.1.5         000f-e234-5679  20       GE1/0/2                5     D
```

Configuration files

```
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface20
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 20
```

```
#
 arp timer aging 5
 arp static 192.168.1.1 00e0-fc01-0000 10 GigabitEthernet1/0/1
#
```

Proxy ARP configuration examples

This chapter provides proxy ARP configuration examples.

Proxy ARP enables hosts on different broadcast domains to communicate with each other as if they were in the same broadcast domain.

Proxy ARP includes common proxy ARP and local proxy ARP.

- **Common proxy ARP**—Allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.
- **Local proxy ARP**—Allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

Example: Configuring common proxy ARP

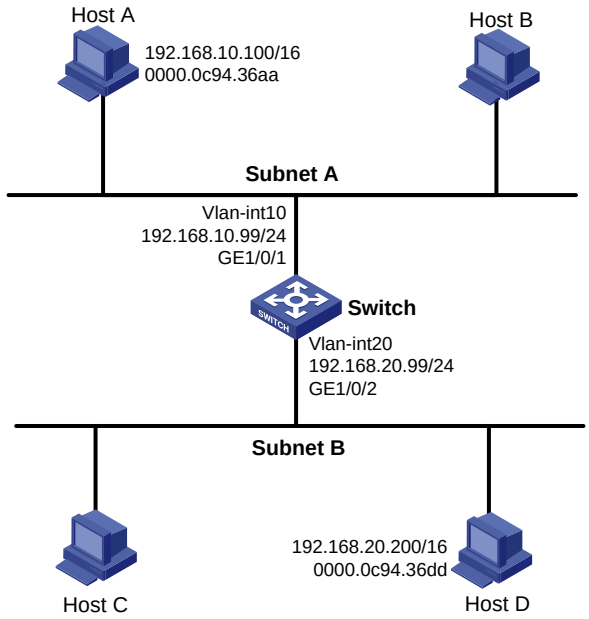
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 48, configure common proxy ARP on the switch to enable communication between Host A and Host D.

Figure 48 Network diagram



Configuration procedures

Create VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
```

Add interface GigabitEthernet 1/0/1 to VLAN 10.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port access vlan 10
[Switch-GigabitEthernet1/0/1] quit
```

Create VLAN-interface 10 and configure its IP address.

```
[Switch] interface vlan-interface 10
[Switch-vlan-interface10] ip address 192.168.10.99 24
[Switch-vlan-interface10] quit
```

Create VLAN 20.

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

Add interface GigabitEthernet 1/0/2 to VLAN 20.

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port access vlan 20
[Switch-GigabitEthernet1/0/2] quit
```

Create VLAN-interface 20 and configure its IP address.

```
[Switch] interface vlan-interface 20
[Switch-vlan-interface20] ip address 192.168.20.99 24
[Switch-vlan-interface20] quit
```

Enable common proxy ARP on interface VLAN-interface 10.

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] proxy-arp enable
[Switch-Vlan-interface10] quit
```

Enable common proxy ARP on interface VLAN-interface 20.

```
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] proxy-arp enable
```

Verifying the configuration

Display the common proxy ARP status on the switch.

```
<Switch> display proxy-arp
Interface Vlan-interface10
 Proxy ARP status: enabled

Interface Vlan-interface20
 Proxy ARP status: enabled
```

Ping Host D from Host A, and ping Host A from Host D. Both ping operations succeed.

Configuration files

```
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.10.99 255.255.255.0
 proxy-arp enable
#
interface Vlan-interface20
 ip address 192.168.20.99 255.255.255.0
 proxy-arp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

Example: Configuring local proxy ARP

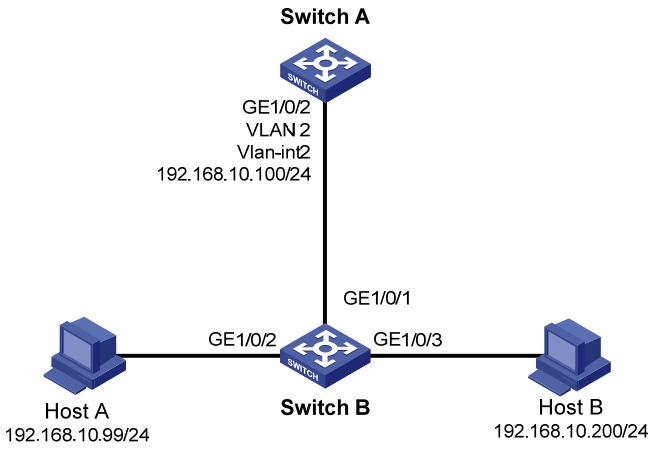
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 49, enable local proxy ARP on Switch A and configure port isolation on Switch B, so that Host A and Host B cannot communicate at Layer 2, but can communicate at Layer 3.

Figure 49 Network diagram



Configuration procedures

1. Configure Switch A:

   # Configure the IP address of interface VLAN-interface 2.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/2
   [SwitchA-vlan2] quit
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.10.100 255.255.255.0
   ```

   # Enable local proxy ARP on interface VLAN-interface 2.

   ```
   [SwitchA-Vlan-interface2] local-proxy-arp enable
   ```

2. Configure Switch B:

   # Add interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

   ```
   <SwitchB> system-view
   ```

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] port gigabitethernet 1/0/3
[SwitchB-vlan2] quit
```

Configure port isolation on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

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

Verifying the configuration

Display local proxy ARP status on Switch A.

```
<SwitchA> display local-proxy-arp
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

Display port isolation information on Switch B.

```
<SwitchB> display port-isolate group
 Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
 Group members:
    GigabitEthernet1/0/2     GigabitEthernet1/0/3
```

Before you enable local proxy ARP on Switch A, Host A cannot ping Host B. Layer 2 isolation is effective. After you enable local proxy ARP on Switch A, Host A can ping Host B. Layer 3 communication is effective.

Configuration files

- Switch A:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.10.100 255.255.255.0
 local-proxy-arp enable
#
interface GigabitEthernet1/0/2
 port access vlan 2
#
```

- Switch B:

```
#
vlan 2
#
```

```
interface GigabitEthernet1/0/1
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port access vlan 2
 port-isolate enable
#
interface GigabitEthernet1/0/3
 port access vlan 2
 port-isolate enable
#
```

Basic MPLS configuration examples

This chapter provides a static LSP configuration example and a dynamic LSP configuration example.

Example: Configuring static LSPs

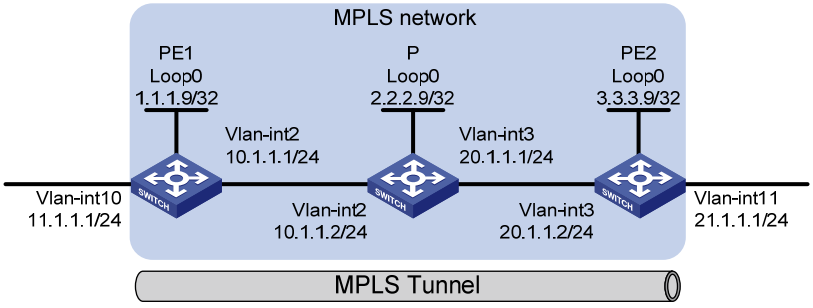
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 50, configure static LSPs between PE 1 and PE 2 so that subnets 11.1.1.1/24 and 21.1.1.1/24 can access each other over MPLS.

Figure 50 Network diagram



Requirements analysis

To make the switches forward MPLS packets along a correct path, make sure the outgoing label specified on an LSR is the same as the incoming label specified on the directly-connected downstream LSR.

LSPs are unidirectional. To make sure data can be bidirectionally forwarded, configure an LSP for each direction of the data forwarding path.

A route to the destination address of the LSP must be available on the ingress node, but it is not required on transit and egress nodes. Therefore, you do not need to configure a routing protocol to ensure IP connectivity among all switches. This example uses a static route.

Configuration restrictions and guidelines

When you configure a static LSP, follow these restrictions and guidelines:

- If you specify a next hop for the static LSP, you must also specify the same next hop in the static IP route configured for the LSP.
- On the ingress or transit node of the static LSP, do not specify the public address of a local interface as the next hop address of the static LSP.
- MPLS adds a label or multiple labels to packets. To prevent MPLS-enabled ports from dropping MPLS packets, enable the jumboframe function and specify a correct jumboframe length on the ports.

Configuration procedures

1. Configure IP addresses for interfaces as shown in Figure 50. (Details not shown.)
2. Configure static routes to make sure the ingress nodes have routes to the destination addresses of the LSPs:

   # Configure PE 1.

   ```
   <PE1> system-view
   [PE1] ip route-static 21.1.1.0 24 10.1.1.2
   ```

   # Configure PE 2.

   ```
   <PE2> system-view
   [PE2] ip route-static 11.1.1.0 24 20.1.1.1
   ```

   # Execute the **display ip routing-table** command on the ingress node to verify that the static route has been created. This example uses PE 1.

   ```
   [PE1] display ip routing-table
   Routing Tables: Public

            Destinations : 8        Routes : 8

   Destination/Mask    Proto  Pre  Cost         NextHop         Interface
   1.1.1.9/32          Direct 0    0            127.0.0.1       InLoop0
   10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
   10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
   11.1.1.0/24         Direct 0    0            11.1.1.1        Vlan10
   11.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
   21.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
   127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
   127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
   ```

3. Enable MPLS:

   # Configure MPLS on PE 1.

   ```
   [PE1] mpls lsr-id 1.1.1.9
   [PE1] mpls
   [PE1-mpls] quit
   [PE1] interface vlan-interface 2
   [PE1-Vlan-interface2] mpls
   [PE1-Vlan-interface2] quit
   ```

Configure MPLS on P.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] mpls
[P-Vlan-interface2] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] mpls
[P-Vlan-interface3] quit
```

Configure MPLS on PE 2.

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] quit
```

4. Create a static LSP from PE 1 to PE 2:

Configure the ingress node PE 1.

```
[PE1] static-lsp ingress PE1_to_PE2 destination 21.1.1.0 24 nexthop 10.1.1.2
out-label 30
```

Configure the transit node P.

```
[P] static-lsp transit PE1_to_PE2 incoming-interface vlan-interface 2 in-label 30
nexthop 20.1.1.2 out-label 50
```

Configure the egress node PE 2.

```
[PE2] static-lsp egress PE1_to_PE2 incoming-interface vlan-interface 3 in-label 50
```

5. Configure a static LSP from PE 2 to PE 1:

Configure the ingress node PE 2.

```
[PE2] static-lsp ingress PE2_to_PE1 destination 11.1.1.0 24 nexthop 20.1.1.1
out-label 40
```

Configure the transit node P.

```
[P] static-lsp transit PE2_to_PE1 incoming-interface vlan-interface 3 in-label 40
nexthop 10.1.1.1 out-label 70
```

Configure the egress node PE 1.

```
[PE1] static-lsp egress PE2_to_PE1 incoming-interface vlan-interface 2 in-label 70
```

Verifying the configuration

Execute the **display mpls static-lsp** command on each switch to view the static LSP information. This example uses PE 1.

```
[PE1] display mpls static-lsp
total statics-lsp : 2
Name            FEC               I/O Label  I/O If                    State
PE1_to_PE2      21.1.1.0/24       NULL/30    -/Vlan2                   Up
PE2_to_PE1      -/-               70/NULL    Vlan2/-                   Up
```

On PE 1, test the connectivity of the LSP from PE 1 to PE 2.

```
[PE1] ping lsp ipv4 21.1.1.0 24
 LSP Ping FEC: LDP IPV4 PREFIX 21.1.1.1/24 : 100  data bytes, press CTRL_C to break
 Reply from 20.1.1.2: bytes=100 Sequence=1 time = 76 ms
 Reply from 20.1.1.2: bytes=100 Sequence=2 time = 75 ms
 Reply from 20.1.1.2: bytes=100 Sequence=3 time = 75 ms
 Reply from 20.1.1.2: bytes=100 Sequence=4 time = 75 ms
 Reply from 20.1.1.2: bytes=100 Sequence=5 time = 75 ms
 --- FEC: LDP IPV4 PREFIX 21.1.1.1/24 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 75/75/76 ms
```

On PE 2, test the connectivity of the LSP from PE 2 to PE 1.

```
[PE2] ping lsp ipv4 11.1.1.0 24
 LSP Ping FEC: LDP IPV4 PREFIX 11.1.1.1/24 : 100  data bytes, press CTRL_C to break
 Reply from 10.1.1.1: bytes=100 Sequence=1 time = 75 ms
 Reply from 10.1.1.1: bytes=100 Sequence=2 time = 75 ms
 Reply from 10.1.1.1: bytes=100 Sequence=3 time = 75 ms
 Reply from 10.1.1.1: bytes=100 Sequence=4 time = 74 ms
 Reply from 10.1.1.1: bytes=100 Sequence=5 time = 75 ms

 --- FEC: LDP IPV4 PREFIX 11.1.1.1/24 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 74/74/75 ms
```

Configuration files

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 10
#
mpls
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
#
interface Vlan-interface10
 ip address 11.1.1.1 255.255.255.0
```

```
#
 ip route-static 21.1.1.0 255.255.255.0 11.1.1.2
#
static-lsp ingress PE1_to_PE2 destination 21.1.1.0 24 nexthop 10.1.1.2 out-label 30
#
static-lsp egress PE2_to_PE1 incoming-interface vlan-interface 2 in-label 70
```

- P:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 3
#
mpls
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface Vlan-interface3
 ip address 20.1.1.1 255.255.255.0
 mpls
#
static-lsp transit PE1_to_PE2 incoming-interface vlan-interface 2 in-label 30 nexthop
20.1.1.2 out-label 50
#
static-lsp transit PE2_to_PE1 incoming-interface vlan-interface 3 in-label 40 nexthop
10.1.1.1 out-label 70
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 11
#
mpls
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 20.1.1.2 255.255.255.0
 mpls
```

```
#
interface Vlan-interface11
 ip address 21.1.1.1 255.255.255.0
#
 ip route-static 11.1.1.0 255.255.255.0 20.1.1.1
#
 static-lsp egress PE1_to_PE2 incoming-interface vlan-interface 3 in-label 50
#
 static-lsp ingress PE2_to_PE1 destination 11.1.1.0 24 nexthop 20.1.1.1 out-label 40
```

Example: Configuring dynamic LSPs through LDP

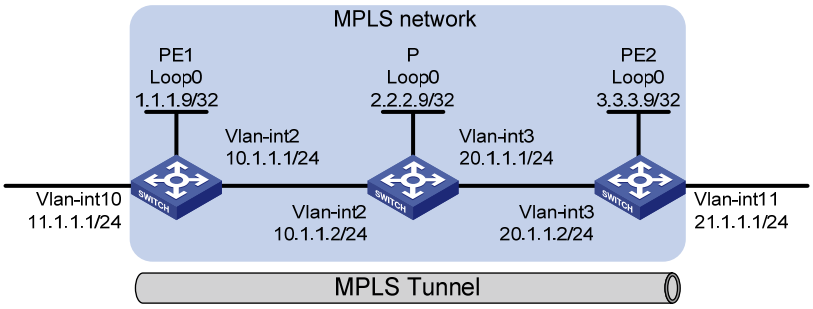
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 51, configure LDP to establish dynamic LSPs between PE 1 and PE 2 so that subnets 11.1.1.1/24 and 21.1.1.1/24 can access each other over MPLS.

Figure 51 Network diagram



Configuration procedures

1. Configure IP addresses for interfaces as shown in Figure 51. (Details not shown.)
2. Configure OSPF to ensure IP connectivity between the switches:

   # Configure OSPF on PE 1.

```
<PE1> system-view
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

```
[PE1-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure OSPF on P.

```
<P> system-view
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configure OSPF on PE 2.

```
<PE2> system-view
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 21.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Execute the **display ip routing-table** command on each switch to verify that each switch has learned the routes to other switches. This example uses PE 1.

```
[PE1] display ip routing-table
Routing Tables: Public

         Destinations : 11        Routes : 11

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.9/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.9/32          OSPF   10   11           10.1.1.2        Vlan2
3.3.3.9/32          OSPF   10   12           10.1.1.2        Vlan2
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
11.1.1.0/24         Direct 0    0            11.1.1.1        Vlan10
11.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         OSPF   10   11           10.1.1.2        Vlan2
21.1.1.0/24         OSPF   10   12           10.1.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

Verify that an OSPF neighbor relationship has been established (in FULL state) between PE 1 and P, and between P and PE 2. This example uses PE 1.

```
[PE1] display ospf peer verbose
          OSPF Process 1 with Switch ID 1.1.1.9
                  Neighbors
 Area 0.0.0.0 interface 10.1.1.1(Vlan-interface10)'s neighbors
 Router ID: 2.2.2.9      Address: 10.1.1.2        GR State: Normal
   State: Full  Mode:Nbr is  Master  Priority: 1
```

```
  DR: None   BDR: None   MTU: 1500
  Dead timer due in 39  sec
  Neighbor is up for 00:02:13
  Authentication Sequence: [ 0 ]
```

3. Enable MPLS and MPLS LDP:

   # Configure MPLS and MPLS LDP on PE 1.

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

   # Configure MPLS and MPLS LDP on P.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

   # Configure MPLS and MPLS LDP on PE 2.

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

   After the configuration is complete, two LDP sessions are established, one between PE 1 and P and the other between P and PE 2.

   # Execute the **display mpls ldp session** command on each switch to view LDP session information. This example uses PE 1.

```
[PE1] display mpls ldp session
               LDP Session(s) in Public Network
 Total number of sessions: 1
 ------------------------------------------------------------
```

```
 Peer-ID       Status        LAM  SsnRole  FT   MD5  KA-Sent/Rcv
 ------------------------------------------------------------------
 2.2.2.9:0     Operational   DU   Passive  Off  Off  5/5
 ------------------------------------------------------------------
 LAM : Label Advertisement Mode         FT  : Fault Tolerance
```

Execute the **display mpls ldp peer** command to view LDP peer information. This example uses PE 1.

```
[PE1] display mpls ldp peer
         LDP Peer Information in Public network
 Total number of peers: 1
------------------------------------------------------------------
 Peer-ID               Transport-Address  Discovery-Source
 ------------------------------------------------------------------
 2.2.2.9:0             2.2.2.9            Vlan-interface10
 ------------------------------------------------------------------
```

4. Allow all routing entries to trigger establishment of LSPs:

Allow all routing entries to trigger establishment of LSPs on PE 1.

```
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
```

Allow all routing entries to trigger establishment of LSPs on P.

```
[P] mpls
[P-mpls] lsp-trigger all
[P-mpls] quit
```

Allow all routing entries to trigger establishment of LSPs on PE 2.

```
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] return
```

Verifying the configuration

Execute the **display mpls ldp lsp** command on each switch to view the LDP LSP information. This example uses PE 1.

```
<PE1> display mpls ldp lsp
                              LDP LSP Information
 -------------------------------------------------------------------------------
 SN     DestAddress/Mask    In/OutLabel   Next-Hop        In/Out-Interface
 -------------------------------------------------------------------------------
 1      1.1.1.9/32          3/NULL        127.0.0.1       -------/InLoop0
 2      2.2.2.9/32          NULL/3        10.1.1.2        -------/Vlan2
 3      3.3.3.9/32          NULL/1027     10.1.1.2        -------/Vlan2
 4      11.1.1.0/24         1029/NULL     0.0.0.0         -------/Vlan10
 5      20.1.1.0/24         NULL/1032     10.1.1.2        -------/Vlan2


 -------------------------------------------------------------------------------
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
```

```
 A '>' before an LSP means the LSP may be inactive
```

On PE 1, test the connectivity of the LDP LSP from PE 1 to PE 2.

```
<PE1> ping lsp ipv4 3.3.3.9 32
 LSP PING FEC: LDP IPV4 PREFIX 3.3.3.9/32 : 100  data bytes, press CTRL_C to break
 Reply from 20.1.1.2: bytes=100 Sequence=1 time = 1 ms
 Reply from 20.1.1.2: bytes=100 Sequence=2 time = 1 ms
 Reply from 20.1.1.2: bytes=100 Sequence=3 time = 1 ms
 Reply from 20.1.1.2: bytes=100 Sequence=4 time = 1 ms
 Reply from 20.1.1.2: bytes=100 Sequence=5 time = 1 ms
 --- FEC: LDP IPV4 PREFIX 3.3.3.9/32 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/1 ms
```

Configuration files

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls
lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface10
 ip address 11.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 11.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
```

- P:

```
#
 mpls lsr-id 2.2.2.9
```

```
#
vlan 2
#
vlan 3
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 11
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 20.1.1.2 255.255.255.0
```

```
 mpls
 mpls ldp
#
interface Vlan-interface11
 ip address 21.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 21.1.1.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
```

BPDU tunneling configuration examples

This chapter provides BPDU tunneling configuration examples.

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

Example: Configuring BPDU tunneling for STP

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

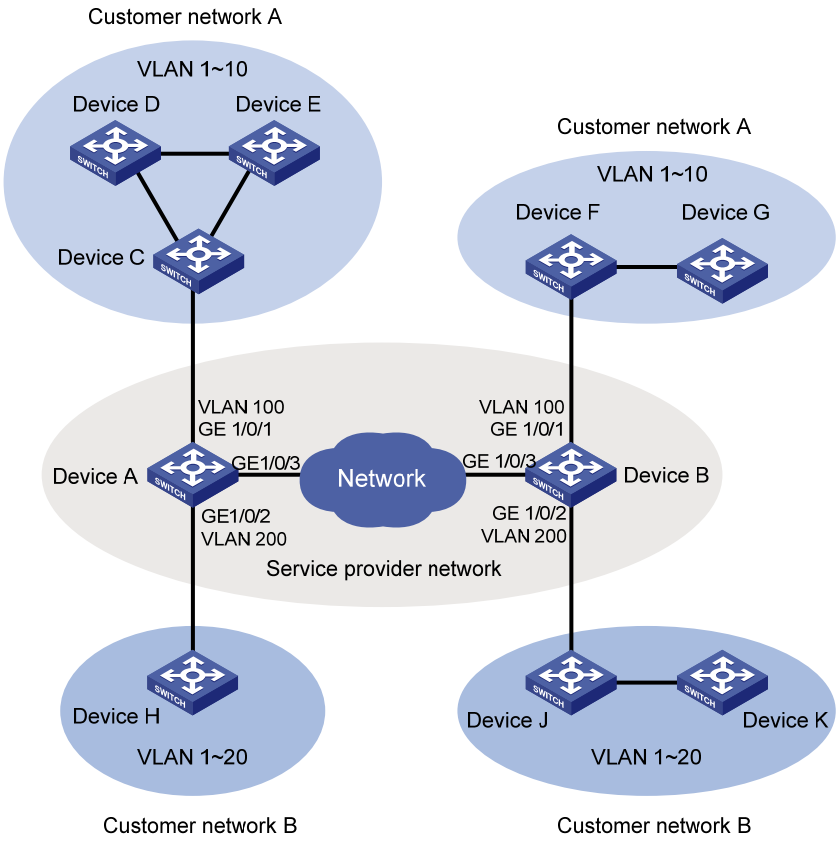
As shown in Figure 52:

- The CVLANs for customer network A are VLANs 1 through 10, and the CVLANs for customer network B are VLANs 1 to 20.
- Basic QinQ is enabled on the customer-side ports of the edge devices Device A and Device B of the service provider network.
- The service provider allocates VLAN 100 and VLAN 200 to serve customer network A and customer network B, respectively.
- MSTP is enabled in the service provider network and customer networks.

Configure BPDU tunneling for STP on Device A and Device B to meet the following requirements:

- Each of the service provider network and customer networks performs an independent spanning tree calculation.
- Each customer network can perform a uniform spanning tree calculation across the service provider network.

Figure 52 Network diagram



Configuration restrictions and guidelines

When you configure BPDU tunneling for STP, follow these restrictions and guidelines:

- Before enabling BPDU tunneling for STP on a port, disable STP on the port first.
- Make sure the VLAN tags of VLAN-tagged BPDUs from the customer network are not modified or removed when the BPDUs are transparently transmitted across the service provider network. Otherwise, the devices cannot transparently transmit the BPDUs from the customer network correctly.

Configuration procedures

Configure Device A

1. Configure GigabitEthernet 1/0/1:

   # Assign port GigabitEthernet 1/0/1 to VLAN 100.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] quit
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port access vlan 100
   ```

   # Enable basic QinQ on the port.

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

Disable STP on the port GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Enable BPDU tunneling for STP on the port.

```
[DeviceA-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
[DeviceA-GigabitEthernet1/0/1] quit
```

2. Configure GigabitEthernet 1/0/2:

Assign port GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceA] vlan 200
[DeviceA-vlan200] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 200
```

Enable basic QinQ on the port.

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

Disable STP on the port GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
```

Enable BPDU tunneling for STP on the port.

```
[DeviceA-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
[DeviceA-GigabitEthernet1/0/2] quit
```

3. Configure GigabitEthernet 1/0/3:

Configure the network-side port GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
```

Assign GigabitEthernet 1/0/3 to VLANs 100 and 200.

```
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

Remove GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring DeviceB

1. Configure GigabitEthernet 1/0/1:

Assign port GigabitEthernet 1/0/1 to VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 100
```

Enable basic QinQ on the port.

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

Disable STP on the port GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Enable BPDU tunneling for STP on the port.

```
[DeviceB-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
[DeviceB-GigabitEthernet1/0/1] quit
```

2. Configure GigabitEthernet 1/0/2:

Assign port GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceB] vlan 200
[DeviceB-vlan200] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 200
```

Enable basic QinQ on the port.

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

Disable STP on the port GigabitEthernet 1/0/2.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

Enable BPDU tunneling for STP on the port.

```
[DeviceB-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configure GigabitEthernet 1/0/3:

Configure the network-side port GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
```

Assign GigabitEthernet 1/0/3 to VLANs 100 and 200.

```
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

Remove GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] quit
```

Verifying the configuration

After the configurations are complete, execute the **display stp bpdu-statistics interface** *interface-type interface-number* command on Device C and Device F to display the following statistics:

- BPDU statistics for the port connecting Device C to Device A.
- BPDU statistics for the port connecting Device F to Device B.

The BPDU statistics show that the two ports can receive STP BPDUs from the peer ends.

Configuration files

- DeviceA:

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 200
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

- DeviceB:

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

CFD configuration examples

This chapter provides Connectivity Fault Detection (CFD) configuration examples.

Use CFD in Layer 2 networks to implement link connectivity detection, fault verification, and fault location.

General configuration restrictions and guidelines

Devices in the same MD must use the same CFD protocol version. Otherwise, they cannot exchange CFD protocol packets.

Example: Configuring CFD

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

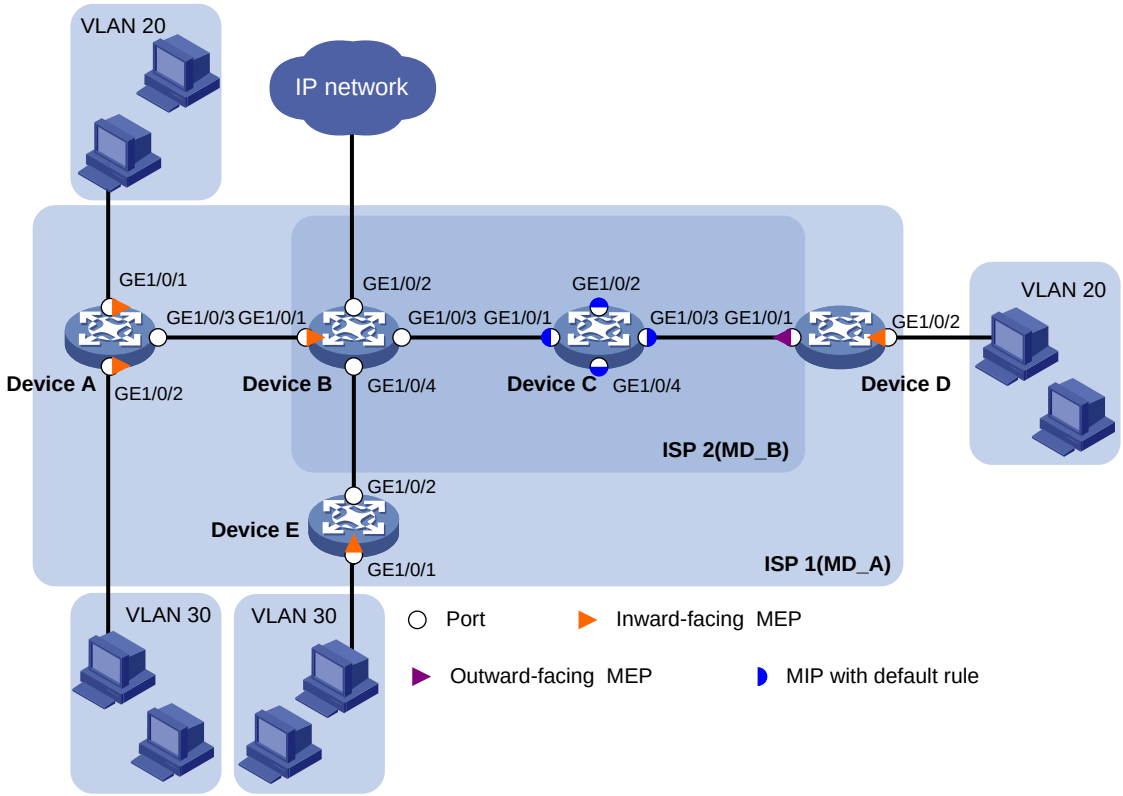
Network requirements

As shown in Figure 53:

- Device A (0010-FC00-6511), Device D (0010-FC00-6514), and Device E (0010-FC00-6515) are managed by ISP 1.
- Device B (0010-FC00-6512) and Device C (0010-FC00-6513) are managed by ISP 2.

Configure CFD to implement link connectivity detection, fault verification, and fault location.

Figure 53 Network diagram



Requirements analysis

To effectively implement CFD:

- Assign devices of an ISP to the same MD.
- Configure a higher level for the outer MD than the nested one.
- Create MAs based on the VLANs of the service traffic.
- In this example, assign ISP 1 to MD_A (level 5) and ISP 2 to MD_B (level 3).

To verify connectivity between MEPs in each MA of MD_A and MD_B, configure the CC function.

Configuration restrictions and guidelines

When you configure CFD, follow these restrictions and guidelines:

- You cannot create a MEP if the MEP ID is not included in the MEP list of the service instance.
- You can configure multiple MAs in an MD as needed. An MA serves only one VLAN.

Configuration procedures

Enabling CFD

Enable CFD on Device A.

```
<DeviceA> system-view
[DeviceA] cfd enable
```

Enable CFD on Device B through Device E. (Details not shown.)

Creating VLANs and assigning ports to the VLANs

Create VLANs and assign ports to the VLANs on the devices. (Details not shown.)

Configuring service instances

Based on the MAs to which the MEPs belong, configure service instances as described in the following table:

Device	MD	MD level	MA	VLAN	Service instance
Device A	MD_A	5	MA_A_1	20	1
			MA_A_2	30	2
Device B	MD_B	3	MA_B_1	20	3
Device C	MD_B	3	MA_B_1	20	3
Device D	MD_A	5	MA_A_1	20	1
	MD_B	3	MA_B_1	20	3
Device E	MD_A	5	MA_A_2	30	2

1. Configure Device A:

   # Create MD_A (level 5).

   ```
   [DeviceA] cfd md MD_A level 5
   ```

   # Create MA_A_1, which serves VLAN 20, in MD_A.

   ```
   [DeviceA] cfd ma MA_A_1 md MD_A vlan 20
   ```

   # Create service instance 1 for MD_A and MA_A_1.

   ```
   [DeviceA] cfd service-instance 1 md MD_A ma MA_A_1
   ```

   # Create MA_A_2, which serves VLAN 30, in MD_A.

   ```
   [DeviceA] cfd ma MA_A_2 md MD_A vlan 30
   ```

   # Create service instance 2 for MD_A and MA_A_2.

   ```
   [DeviceA] cfd service-instance 2 md MD_A ma MA_A_2
   ```

   Configure Device B through Device E in the same way Device A is configured.

2. Configure Device B:

   ```
   [DeviceB] cfd md MD_B level 3
   [DeviceB] cfd ma MA_B_1 md MD_B vlan 20
   [DeviceB] cfd service-instance 3 md MD_B ma MA_B_1
   ```

3. Configure Device C:

   ```
   [DeviceC] cfd md MD_B level 3
   [DeviceC] cfd ma MA_B_1 md MD_B vlan 20
   [DeviceC] cfd service-instance 3 md MD_B ma MA_B_1
   ```

4. Configure Device D:

   ```
   [DeviceD] cfd md MD_A level 5
   [DeviceD] cfd ma MA_A_1 md MD_A vlan 20
   [DeviceD] cfd service-instance 1 md MD_A ma MA_A_1
   [DeviceD] cfd md MD_B level 3
   [DeviceD] cfd ma MA_B_1 md MD_B vlan 20
   ```

```
[DeviceD] cfd service-instance 3 md MD_B ma MA_B_1
```

5. Configure Device E:

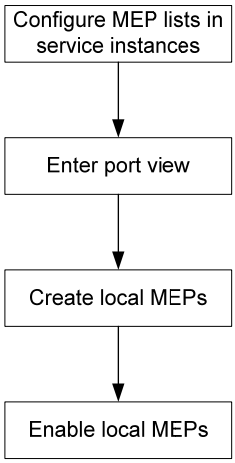
```
[DeviceE] cfd md MD_A level 5
[DeviceE] cfd ma MA_A_2 md MD_A vlan 30
[DeviceE] cfd service-instance 2 md MD_A ma MA_A_2
```

Configuring MEPs

Assign MEP IDs as described in the following table:

Service instance	Device	Port	MEP ID	MEP type
1	Device A	GigabitEthernet 1/0/1	1001	Inward-facing MEP
	Device D	GigabitEthernet 1/0/2	1002	Inward-facing MEP
2	Device A	GigabitEthernet 1/0/2	2001	Inward-facing MEP
	Device E	GigabitEthernet 1/0/1	2002	Inward-facing MEP
3	Device B	GigabitEthernet 1/0/1	3001	Inward-facing MEP
	Device D	GigabitEthernet 1/0/1	3002	Outward-facing MEP

Figure 54 MEP configuration procedure



1. Configure Device A:

Configure a MEP list in service instances 1 and 2.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] cfd meplist 2001 2002 service-instance 2
```

Create and enable inward-facing MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Create and enable inward-facing MEP 2001 in service instance 2 on GigabitEthernet 1/0/2.

```
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 inbound
[DeviceA-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure Device B, Device D, and Device E in the same way Device A is configured.

2. Configure Device B:

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 3001 service-instance 3 inbound
[DeviceB-GigabitEthernet1/0/1] cfd mep service-instance 3 mep 3001 enable
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure Device D:

```
[DeviceD] cfd meplist 1001 1002 service-instance 1
[DeviceD] cfd meplist 3001 3002 service-instance 3
[DeviceD] interface GigabitEthernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 1002 service-instance 1 inbound
[DeviceD-GigabitEthernet1/0/2] cfd mep service-instance 1 mep 1002 enable
[DeviceD-GigabitEthernet1/0/2] quit
[DeviceD] interface GigabitEthernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 3002 service-instance 3 outbound
[DeviceD-GigabitEthernet1/0/1] cfd mep service-instance 3 mep 3002 enable
[DeviceD-GigabitEthernet1/0/1] quit
```

4. Configure Device E:

```
[DeviceE] cfd meplist 2001 2002 service-instance 2
[DeviceE] interface GigabitEthernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd mep 2002 service-instance 2 inbound
[DeviceE-GigabitEthernet1/0/1] cfd mep service-instance 2 mep 2002 enable
[DeviceE-GigabitEthernet1/0/1] quit
```

Configuring a MIP generation rule

MIP configuration is optional. MIPs process LTM frames and LBM frames, and can help implement link fault identification and location.

Configure the MIP generation rule in service instance 3 on Device C as the default.

```
[DeviceC] cfd mip-rule default service-instance 3
```

Configuring CC on MEPs

1. Configure Device A:

   # Enable the sending of CCM frames for MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Enable the sending of CCM frames for MEP 2001 in service instance 2 on GigabitEthernet 1/0/2.

```
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

   Configure Device B, Device D, and Device E in the same way Device A is configured.

2. Configure Device B:

```
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3001 enable
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure Device D:

```
[DeviceD] interface GigabitEthernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3002 enable
[DeviceD-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 1 mep 1002 enable
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure Device E:

```
[DeviceE] interface GigabitEthernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 2002 enable
[DeviceE-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display information about remote MEP 1001 in service instance 1 on Device A.

```
[DeviceA] display cfd remote-mep service-instance 1 mep 1001
MEP ID   MAC Address      State        Time                 MAC Status
1002     0010-FC00-6514   OK           2013/02/01 12:54:52  UP
```

The remote MEP is operating correctly.

Enable LB on Device A to check the status of the link between MEP 1001 and MEP 1002 in service instance 1.

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 1002
Loopback to 0010-FC00-6514 with the sequence number start from 1001-43404:
Reply from 0010-FC00-6514: sequence number=1001-43404
Reply from 0010-FC00-6514: sequence number=1001-43405
Reply from 0010-FC00-6514: sequence number=1001-43406
Reply from 0010-FC00-6514: sequence number=1001-43407
Reply from 0010-FC00-6514: sequence number=1001-43408
Send:5        Received:5        Lost:0
```

The output shows that no link fault occurs on the link between MEP 1001 and MEP 1002 in service instance 1.

Identify the path between MEP 3001 and MEP 3002 in service instance 3 on Device B.

```
[DeviceB] cfd linktrace service-instance 3 mep 3001 target-mep 3002
Linktrace to MEP 3002 with the sequence number 3001-34
MAC Address               TTL     Last MAC         Relay Action
0010-FC00-6513            63      0010-FC00-6512   FDB
0010-FC00-6514            62      0010-FC00-6513   Hit
```

The output shows that MEP 3001 locates MEP 3002 in service instance 3. After receiving LTM messages from the source MEP, MIPs on the path and the target MEP send LTR messages to the source MEP. The source MEP then identifies the path between MEP 3001 and MEP 3002.

Configuration files

- Device A:

```
#
 cfd enable
```

```
 cfd md MD_A level 5
 cfd ma MA_A_1 md MD_A vlan 20
 cfd service-instance 1 md MD_A ma MA_A_1
 cfd meplist 1001 to 1002 service-instance 1
 cfd ma MA_A_2 md MD_A vlan 30
 cfd service-instance 2 md MD_A ma MA_A_2
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 20
#
vlan 30
#
interface GigabitEthernet1/0/1
 port access vlan 20
 cfd mep 1001 service-instance 1 inbound
 cfd mep service-instance 1 mep 1001 enable
 cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
 port access vlan 30
 cfd mep 2001 service-instance 2 inbound
 cfd mep service-instance 2 mep 2001 enable
 cfd cc service-instance 2 mep 2001 enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 20 30
```

- Device B:

```
#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_B_1 md MD_B vlan 20
 cfd service-instance 3 md MD_B ma MA_B_1
 cfd meplist 3001 to 3002 service-instance 3
#
vlan 20
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 20 30
 cfd mep 3001 service-instance 3 inbound
 cfd mep service-instance 3 mep 3001 enable
 cfd cc service-instance 3 mep 3001 enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
```

```
 port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 30
```

- Device C:

```
#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_B_1 md MD_B vlan 20
 cfd service-instance 3 md MD_B ma MA_B_1
 cfd mip-rule default service-instance 3
#
vlan 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 30
```

- Device D:

```
#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_B_1 md MD_B vlan 20
 cfd service-instance 3 md MD_B ma MA_B_1
 cfd meplist 3001 to 3002 service-instance 3
 cfd md MD_A level 5
 cfd ma MA_A_1 md MD_A vlan 20
 cfd service-instance 1 md MD_A ma MA_A_1
 cfd meplist 1001 to 1002 service-instance 1
#
vlan 20
#
```

```
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 20
 cfd mep 3002 service-instance 3 outbound
 cfd mep service-instance 3 mep 3002 enable
 cfd cc service-instance 3 mep 3002 enable
#
interface GigabitEthernet1/0/2
 port access vlan 20
 cfd mep 1002 service-instance 1 inbound
 cfd mep service-instance 1 mep 1002 enable
 cfd cc service-instance 1 mep 1002 enable
```

- Device E:

```
#
 cfd enable
 cfd md MD_A level 5
 cfd ma MA_A_2 md MD_A vlan 30
 cfd service-instance 2 md MD_A ma MA_A_2
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 30
#
interface GigabitEthernet1/0/1
 port access vlan 30
 cfd mep 2002 service-instance 2 inbound
 cfd mep service-instance 2 mep 2002 enable
 cfd cc service-instance 2 mep 2002 enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 30
```

DHCP configuration examples

This chapter provides DHCP configuration examples.

Example: Configuring the DHCP server

Applicable product matrix

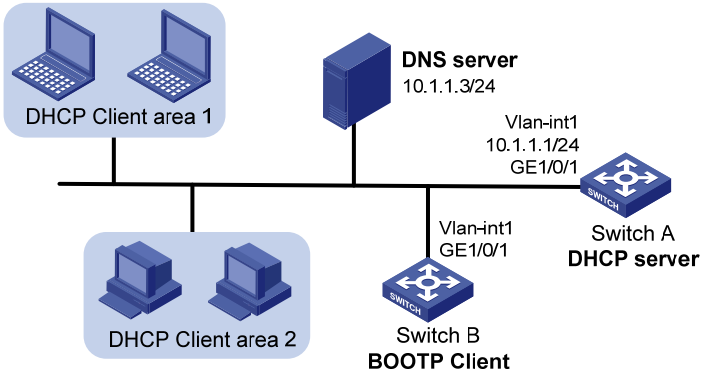
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 55, configure the DHCP server on Switch A to implement the following:

- Dynamically assign IP addresses, lease duration, DNS information, and gateway addresses to DHCP clients in subnet 10.1.1.0/24.
- Assign IP address, DNS information, and gateway address to Switch B according to the MAC address of Switch B.
- Detect unauthorized DHCP servers in the network.

Figure 55 Network diagram



Requirements analysis

To make sure the IP address of the DNS server is not assigned to any client by the DHCP server, you must exclude it from dynamic address allocation.

To enable administrators to locate unauthorized DHCP servers, you must enable the unauthorized DHCP server detection on the DHCP server. The server then records the IP address of all DHCP servers that assign IP addresses to clients and the interfaces that receive DHCP message.

Configuration restrictions and guidelines

To ensure correct address allocation, keep the IP addresses used for dynamic allocation in the subnet where the interface of the DHCP server resides as possible as you can.

Configuration procedures

Specify an IP address for VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.1.1.1 24
```

Enable DHCP.

```
[SwitchA] dhcp enable
```

Enable DHCP server on VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp select server global-pool
[SwitchA-Vlan-interface1] quit
```

Exclude the IP address of the DNS server from address allocation.

```
[SwitchA] dhcp server forbidden-ip 10.1.1.3
```

Configure DHCP address pool 0.

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] static-bind mac-address 000f-e249-8050
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.6 24
[SwitchA-dhcp-pool-0] dns-list 10.1.1.3
[SwitchA-dhcp-pool-0] domain-name com
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.1
[SwitchA-dhcp-pool-0] quit
```

Configure DHCP address pool 1.

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] dns-list 10.1.1.3
[SwitchA-dhcp-pool-1] domain-name com
[SwitchA-dhcp-pool-1] expired day 10
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.1
[SwitchA-dhcp-pool-1] quit
```

Enable unauthorized DHCP server detection.

```
[SwitchA] dhcp server detect
```

Verifying the configuration

After the configuration is completed, verify that the clients can obtain IP addresses and configuration parameters from Switch A.

Use the **display** commands to verify the DHCP information. For example, use the **display dhcp server tree** command to display DHCP address pool information.

```
[SwitchA] display dhcp server tree all
```

```
Global pool:

Pool name: 0
 static-bind ip-address 10.1.1.6 mask 255.255.255.0
 static-bind mac-address 000f-e249-8050
 Parent node:1
 gateway-list 10.1.1.1
 dns-list 10.1.1.3
 domain-name com
 expired unlimited

Pool name: 1
 network 10.1.1.0 mask 255.255.255.0
 Child node:0
 gateway-list 10.1.1.1
 dns-list 10.1.1.3
 domain-name com
 expired 10 0 0 0
```

Use the **dhcp server ip-in-use** command to display IP-to-MAC binding information.

```
[SwitchA] display dhcp server ip-in-use all
Pool utilization: 1.18%
 IP address       Client-identifier/    Lease expiration          Type
                  Hardware address
 10.1.1.6         000f-e249-8050        NOT Used                  Manual
 10.1.1.2         3822-d63a-e106        May  3 2013 09:53:48     Auto:COMMITTED
 10.1.1.4         3363-6535-2e61-3664-  May  3 2013 09:54:10     Auto:COMMITTED
                  662e-6531-3339-2d56-
                  6c61-6e2d-696e-7465-
                  7266-6163-6531

 --- total 3 entry ---
```

Configuration files

```
#
vlan 1
#
dhcp server ip-pool 0
 static-bind ip-address 10.1.1.6 mask 255.255.255.0
 static-bind mac-address 000f-e249-8050
 gateway-list 10.1.1.1
 dns-list 10.1.1.3
 domain-name com
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
 gateway-list 10.1.1.1
 dns-list 10.1.1.3
```

```
 domain-name com
 expired day 10
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
#
 dhcp server forbidden-ip 10.1.1.3
 dhcp server detect
#
 dhcp enable
#
```

Example: Configuring the DHCP relay agent

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

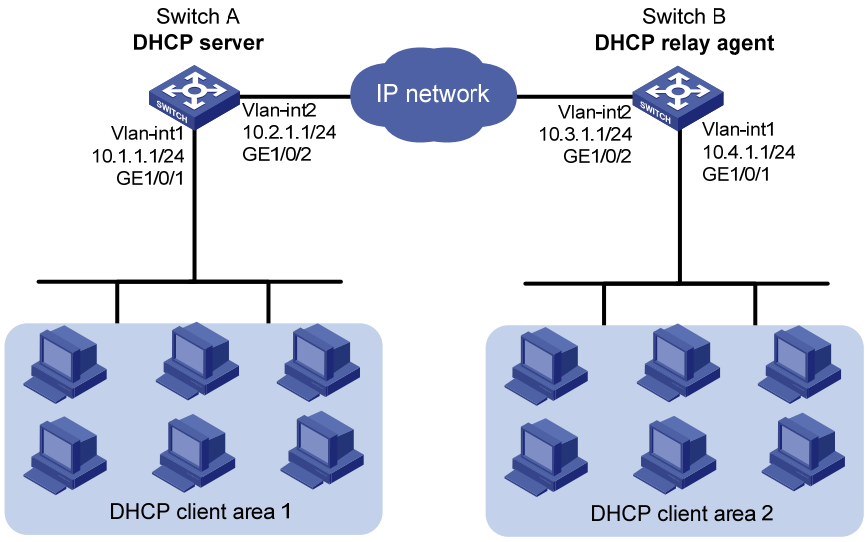
Network requirements

As shown in Figure 56, Switch A and Switch B can reach each other. The DHCP server (Switch A) assigns IP addresses to clients in area 1.

Perform the following tasks to implement DHCP relay:

- Configure the DHCP relay agent on Switch B so that the DHCP server can assign IP addresses to DHCP clients in area 2.
- Enable address check on the DHCP relay agent so DHCP clients in area 2 cannot use manually configured static IP addresses to communicate with the external network.

Figure 56 Network diagram



Requirements analysis

To prevent hosts from using manually configured IP addresses to access the external network, you must enable address check on the DHCP relay agent.

Configuration restrictions and guidelines

When you configure DHCP relay agent, follow these restrictions and guidelines:.

- To make sure the DHCP clients to obtain correct IP addresses through the DHCP relay agent, you must configure an IP address pool that contains the IP address of the DHCP relay agent on the DHCP server.
- The IP address of the DHCP server must not reside on the same subnet as the IP address of the relay agent interface. Otherwise, the clients might fail to obtain IP addresses.
- Before enabling address check on an interface, enable the DHCP service and the DHCP relay agent on the interface. Otherwise, the address check configuration does not take effect.

Configuration procedures

Configuring Switch A

Specify IP addresses for VLAN interfaces.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.1.1.1 24
[SwitchA-Vlan-interface1] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port GigabitEthernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.2.1.1 24
```

```
[SwitchA-Vlan-interface2] quit
```

Enable DHCP.

```
[SwitchA] dhcp enable
```

Configure DHCP address pool 0.

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] quit
```

Configure DHCP address pool 1.

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.4.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] quit
```

Configuring Switch B

Specify IP addresses for VLAN interfaces.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.4.1.1 24
[SwitchB-Vlan-interface1] quit
[SwitchB] vlan 2
[SwitchB-vlan2] port GigabitEthernet 1/0/2
[SwitchB-vlan2] quit
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.3.1.1 24
[SwitchB-Vlan-interface2] quit
```

Enable DHCP.

```
[SwitchB] dhcp enable
```

Specify DHCP server 10.2.1.1 for DHCP server group 1 on the relay agent.

```
[SwitchB] dhcp relay server-group 1 ip 10.2.1.1
```

Enable the DHCP relay agent on VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] dhcp select relay
```

Apply DHCP server group 1 to VLAN-interface 1.

```
[SwitchB-Vlan-interface1] dhcp relay server-select 1
```

Enable address check on the relay agent.

```
[SwitchB-Vlan-interface1] dhcp relay address-check enable
```

Verifying the configuration

After the configuration is completed, verify that the clients in area 1 and area 2 can obtain IP addresses and configuration parameters from Switch A.

Use the **display** commands to verify the DHCP relay agent information on Switch B. For example, use the **display dhcp relay all** command to display DHCP server groups.

```
[SwitchB] display dhcp relay all
    Interface name                                Server-group
    Vlan-interface1                                     1
```

Configuration files

- Switch A:

```
#
vlan 1
#
vlan 2
#
dhcp server ip-pool 0
 network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 1
 network 10.4.1.0 mask 255.255.255.0
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface2
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
 port access vlan 2
#
dhcp enable
#
```

- Switch B:

```
#
 dhcp relay server-group 1 ip 10.2.1.1
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 10.4.1.1 255.255.255.0
 dhcp select relay
 dhcp relay address-check enable
 dhcp relay server-select 1
#
interface Vlan-interface2
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
 port access vlan 2
```

```
#
dhcp enable

#
```

Example: Configuring DHCP relay agent support for Option 82

Applicable product matrix

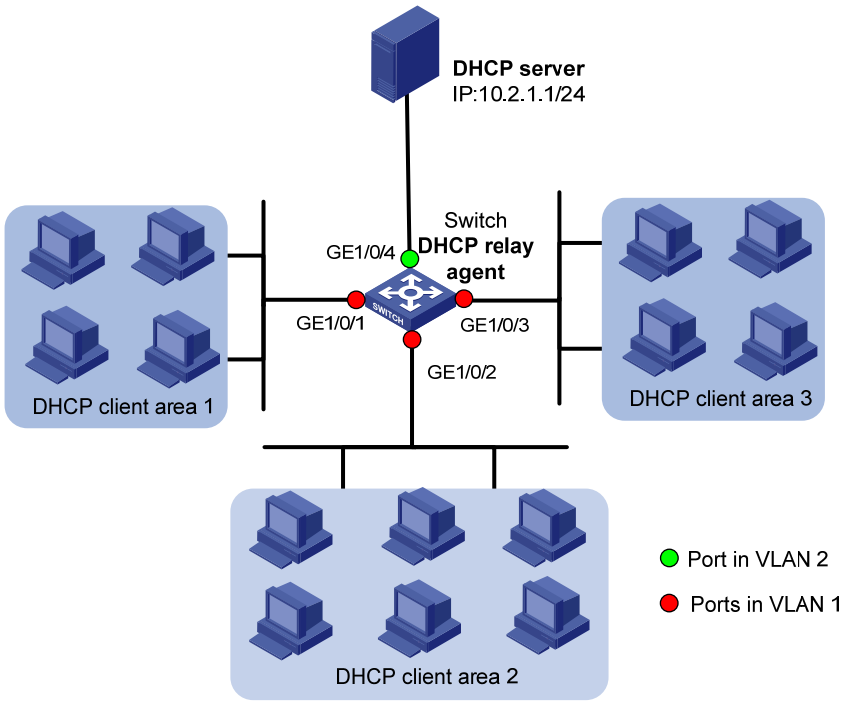
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 57, Option 82 configuration is completed on the DHCP server.

Configure the DHCP relay agent to support Option 82 so the DHCP server can assign IP addresses in specific ranges to DHCP clients in different areas.

Figure 57 Network diagram



Configuration procedures

Specify IP addresses for VLAN interfaces.

```
<Switch> system-view
[Switch] interface Vlan-interface 1
[Switch-Vlan-interface1] ip address 10.1.1.1 24
[Switch-Vlan-interface1] quit
[Switch] vlan 2
[Switch-vlan2] port GigabitEthernet 1/0/4
[Switch-vlan2] quit
[Switch] interface Vlan-interface 2
[Switch-Vlan-interface2] ip address 10.2.1.2 24
[Switch-Vlan-interface2] quit
```

Enable DHCP.

```
[Switch] dhcp enable
```

Specify DHCP server 10.2.1.1 for DHCP server group 1 on the relay agent.

```
[Switch] dhcp relay server-group 1 ip 10.2.1.1
```

Enable the DHCP relay agent on VLAN-interface 1.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] dhcp select relay
```

Apply DHCP server group 1 to VLAN-interface 1.

```
[Switch-Vlan-interface1] dhcp relay server-select 1
```

Enable the DHCP relay agent to support Option 82.

```
[Switch-Vlan-interface1] dhcp relay information enable
```

Verifying the configuration

After the configuration is completed, verify that DHCP clients can obtain IP addresses on specific subnets from the DHCP server.

Use the **display dhcp relay information** command to display Option 82 configuration on the DHCP relay agent.

```
[Switch] display dhcp relay information all
Interface: Vlan-interface1
    Status: Enable
    Strategy: Replace
    Format: Normal
```

Configuration files

```
#
 dhcp relay server-group 1 ip 10.2.1.1
#
vlan 1
#
vlan 2
```

```
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
 dhcp relay information enable
#
interface Vlan-interface2
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
 port access vlan 2
#
 dhcp enable
#
```

Example: configuring DHCP snooping

Applicable product matrix

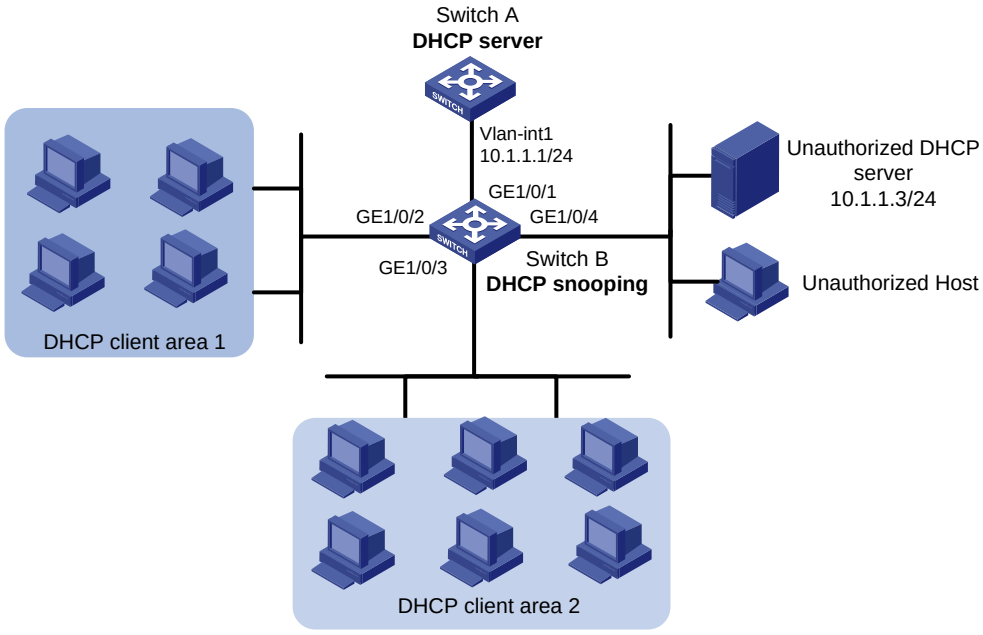
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 58, configure DHCP snooping on Switch B to implement the following:

- Make sure DHCP clients obtain IP addresses from the authorized DHCP server (Switch A).
- Prevent users from accessing the network through static IP addresses.

Figure 58 Network diagram



Requirements analysis

To make sure Switch B forward DHCP messages from the authorized DHCP server to DHCP clients, you must configure GigabitEthernet 1/0/1 as trusted and configure other ports as untrusted.

To prevent users from accessing the network through static IP addresses, you must enable ARP detection in VLAN 1 for user validity check.

Configuration procedures

Configuring Switch A

Specify an IP address for VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.1.1.1 24
```

Enable DHCP.

```
[SwitchA] dhcp enable
```

Configure DHCP address pool 0.

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] quit
```

Configuring Switch B

Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

Specify GigabitEthernet 1/0/1 as a trusted port.

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Enable ARP detection for user validity check.

```
[SwitchB] vlan 1
[SwitchB-vlan1] arp detection enable
```

Specify GigabitEthernet 1/0/1 as ARP trusted port. By default, a port is an ARP untrusted port.

```
[SwitchB-vlan1] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp detection trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display DHCP snooping entries.

```
[SwitchB] display dhcp-snooping
 DHCP Snooping is enabled.
The client binding table for all ports.
 Type : D--Dynamic , S--Static , R--Recovering
 Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
 ==== =============== ============== ============ ==== ===== =================
 D    10.1.1.15       00e0-fc00-0006 286          1    N/A   Gigabitethernet1/0/1
---   1 dhcp-snooping item(s) found   ---
```

Configuration files

- Switch A:

```
#
vlan 1
#
dhcp server ip-pool 0
 network 10.1.1.0 mask 255.255.255.0
#
 dhcp enable
#
```

- Switch B:

```
#
 dhcp-snooping
#
vlan 1
 arp detection enable
#
interface GigabitEthernet1/0/1
 dhcp-snooping trust
 arp detection trust
#
```

DLDP configuration examples

This document provides DLDP configuration examples.

The Device Link Detection Protocol (DLDP) is developed by HP. DLDP detects unidirectional links (fiber links or twisted-pair links). When DLDP detects unidirectional links, it can automatically shut down the faulty port or users can manually shut down the faulty port to avoid network problems.

Example: Automatically shutting down unidirectional links

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620
	Release series 6630
	Release series 6700

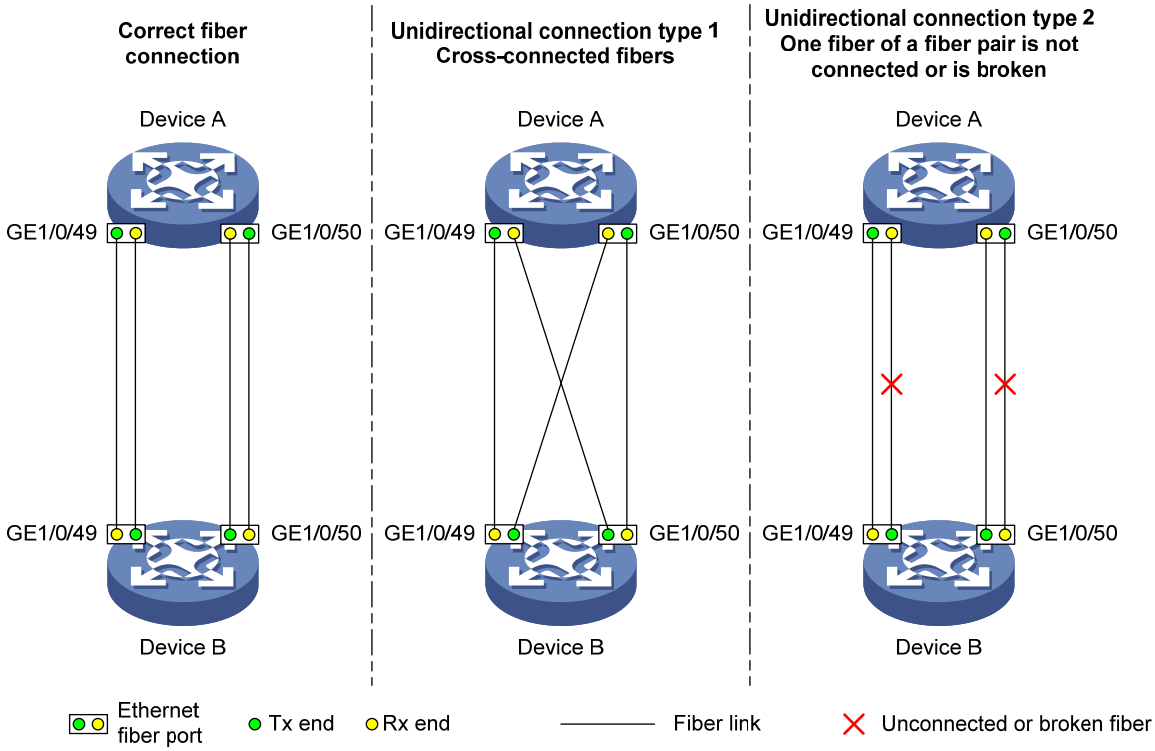
Network requirements

As shown in Figure 59, Device A and Device B are connected with two fiber pairs.

Configure DLDP on the devices to meet these requirements:

- Detect unidirectional links caused by cross-connected fibers or a disconnected fiber or open circuit condition.
- Automatically shut down the faulty port when detecting a unidirectional link.
- Automatically bring up the port after the administrator clears the fault.

Figure 59 Network diagram



Configuration restrictions and guidelines

When you configure DLDP, follow these restrictions and guidelines:

- To make sure DLDP operates correctly on a link, you must configure the full duplex mode for the ports at two ends of the link, and configure a speed for the two ports.
- The default DLDP mode is normal, and the system can detect only unidirectional links caused by cross-connected fibers. Set the DLDP mode to enhanced to enable DLDP to detect unidirectional links caused by one of the following conditions:
  - Cross-connected fibers.
  - Disconnected fiber.
  - Open circuit condition..

Configuration procedures

1. Configure Device A:

   # Enable DLDP globally.

   ```
   <DeviceA> system-view
   [DeviceA] dldp enable
   ```

   # Configure GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 to operate in full duplex mode at 1000 Mbps, and enable DLDP on the ports.

   ```
   [DeviceA] interface gigabitethernet 1/0/49
   [DeviceA-GigabitEthernet1/0/49] duplex full
   [DeviceA-GigabitEthernet1/0/49] speed 1000
   ```

```
[DeviceA-GigabitEthernet1/0/49] dldp enable
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] duplex full
[DeviceA-GigabitEthernet1/0/50] speed 1000
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
```

Set the DLDP mode to enhanced.

```
[DeviceA] dldp work-mode enhance
```

Set the port shutdown mode to auto.

```
[DeviceA] dldp unidirectional-shutdown auto
```

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

Verifying the configuration

After the configurations are complete, you can use the **display dldp** command to display the DLDP configuration information on ports.

Display the DLDP configuration information about all the DLDP-enabled ports of Device A.

```
[DeviceA] display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : none
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 1s
 The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 59
         Neighbor state : two way
         Neighbor aged time : 11

Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 60
         Neighbor state : two way
         Neighbor aged time : 12
```

The output shows that both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 are in Advertisement state, which means both links are bidirectional.

Enable system information monitoring on Device A, and enable the display of log and trap information.

```
[DeviceA] quit
<DeviceA> terminal monitor
Info: Current terminal monitor is on.
<DeviceA> terminal logging
Info: Current terminal logging is on.
<DeviceA> terminal trapping
Info: Current terminal trapping is on.
```

If the two pairs of fibers between Device A and Device B are cross-connected, the following log and trap information is displayed on Device A:

```
<DeviceA>
#Jan 18 17:36:18:798 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825792.

%Jan 18 17:36:18:799 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link
status is DOWN.
%Jan 18 17:36:18:799 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/49. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.
#Jan 18 17:36:20:189 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825793.

%Jan 18 17:36:20:189 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link
status is DOWN.
%Jan 18 17:36:20:190 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/50. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.

%Jan 15 16:54:56:040 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO_ENHANCE: -Slot=1; In
enhanced DLDP mode, port GigabitEthernet1/0/49 cannot detect its aged-out neighbor.
The transceiver has malfunction in the Tx direction or cross-connected links exist
between the local device and its neighbor. The shutdown mode is AUTO. DLDP shuts down
the port.
```

The output shows the following information:

- The link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is down.
- DLDP has detected a unidirectional link on both ports and has automatically shut them down.

Correct the fiber connections. As a result, the ports shut down by DLDP automatically recover, and Device A displays the following log information:

```
<DeviceA>
%Jan 18 17:47:33:869 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link
status is UP.
%Jan 18 17:47:35:894 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link
status is UP.
```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is now up.

Configuration files

- Device A:

```
#
 dldp enable
 dldp work-mode enhance
#
interface GigabitEthernet1/0/49
 speed 1000
 duplex full
 dldp enable
#
interface GigabitEthernet1/0/50
 speed 1000
 duplex full
 dldp enable
#
```

- Device B:

  The configuration files on Device B are the same as those on Device A. (Details not shown.)

Example: Manually shutting down unidirectional links

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

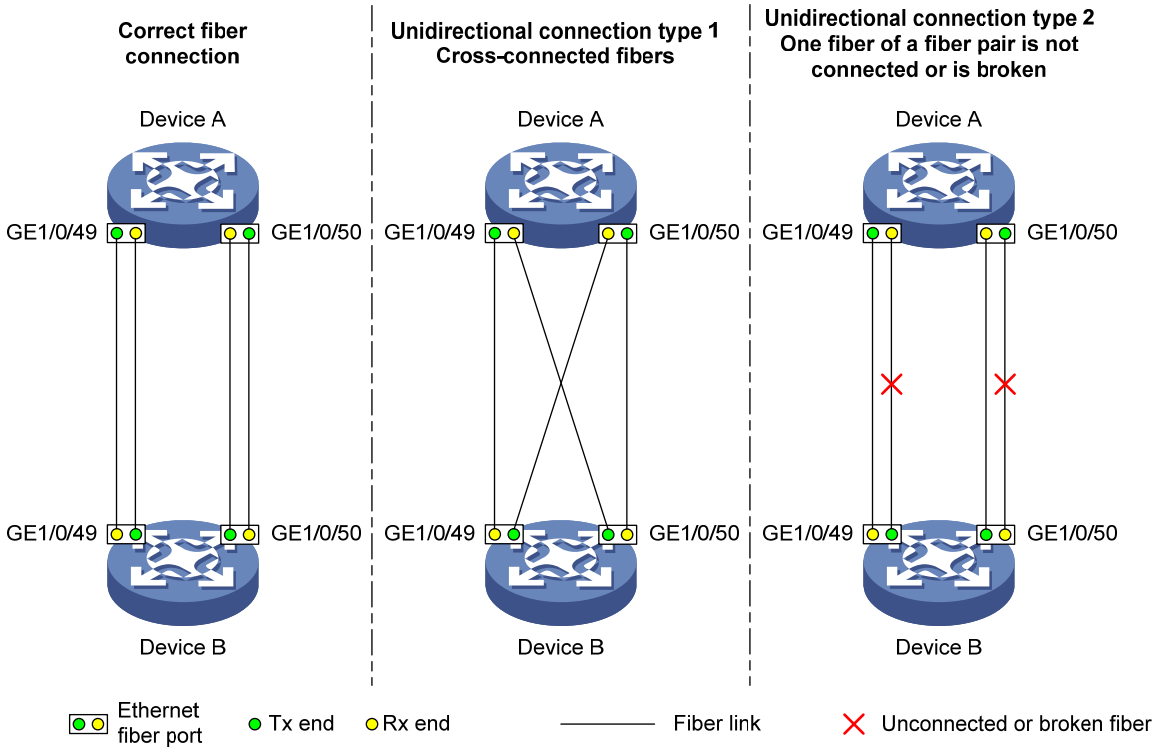
Network requirements

As shown in Figure 60, Device A and Device B are connected with two fiber pairs.

Configure DLDP on the devices to meet these requirements:

- Detect unidirectional links caused by cross-connected fibers or a disconnected fiber or open circuit condition.
- When a unidirectional link is detected, the administrator must manually shut down the port.
- The administrator must manually bring up the port after clearing the fault.

Figure 60 Network diagram



Configuration restrictions and guidelines

When you configure DLDP, follow these restrictions and guidelines:

- To make sure DLDP operates correctly on a link, you must configure the full duplex mode for the ports at two ends of the link. You must also configure a speed for the two ports.
- The default DLDP mode is normal, and the system can detect only unidirectional links caused by cross-connected fibers. Set the DLDP mode to enhanced to enable DLDP to detect unidirectional links caused by one of the following conditions:
  - Ccross-connected fibers.
  - Disconnected fiber.
  - Open circuit condition.

Configuration procedures

1. Configure Device A:

   # Enable DLDP globally.

   ```
   <DeviceA> system-view
   [DeviceA] dldp enable
   ```

   # Configure GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 to operate in full duplex mode at 1000 Mbps, and enable DLDP on the ports.

   ```
   [DeviceA] interface gigabitethernet 1/0/49
   [DeviceA-GigabitEthernet1/0/49] duplex full
   [DeviceA-GigabitEthernet1/0/49] speed 1000
   ```

```
[DeviceA-GigabitEthernet1/0/49] dldp enable
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] duplex full
[DeviceA-GigabitEthernet1/0/50] speed 1000
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
```

Set the DLDP mode to enhanced.

```
[DeviceA] dldp work-mode enhance
```

Set the port shutdown mode to manual.

```
[DeviceA] dldp unidirectional-shutdown manual
```

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

Verifying the configuration

After the configurations are complete, you can use the **display dldp** command to display the DLDP configuration information on ports.

Display the DLDP configuration information on all the DLDP-enabled ports of Device A.

```
[DeviceA] display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : none
 DLDP unidirectional-shutdown : manual
 DLDP delaydown-timer : 1s
 The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 59
         Neighbor state : two way
         Neighbor aged time : 11

Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 60
         Neighbor state : two way
         Neighbor aged time : 12
```

The output shows that both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 are in Advertisement state, which means both links are bidirectional.

Enable system information monitoring on Device A, and enable the display of log and trap information.

```
[DeviceA] quit
<DeviceA> terminal monitor
Info: Current terminal monitor is on.
<DeviceA> terminal logging
Info: Current terminal logging is on.
<DeviceA> terminal trapping
Info: Current terminal trapping is on.
```

If the two pairs of fibers between Device A and Device B are cross-connected, the following log and trap information is displayed on Device A:

```
<DeviceA>
#Jan 18 18:10:38:481 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825792.

%Jan 18 18:10:38:481 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/49. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is MANUAL. The port needs to be shut down by the
user.
#Jan 18 18:10:38:618 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825793.

%Jan 18 18:10:38:618 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/50. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is MANUAL. The port needs to be shut down by the
user.
```

The output shows that DLDP has detected a unidirectional link on both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50. You are prompted to manually shut down the faulty ports.

After you shut down GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50, the following log information is displayed:

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] shutdown
%Jan 18 18:16:12:044 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link
status is DOWN.
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] shutdown
%Jan 18 18:18:03:583 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link
status is DOWN.
```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is down.

In this example, the unidirectional links are caused by cross-connected fibers. Correct the fiber connections, and then bring up the ports previously shut down.

On Device A, bring up GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50:

```
[DeviceA-GigabitEthernet1/0/50] undo shutdown
[DeviceA-GigabitEthernet1/0/50]
%Jan 18 18:22:11:698 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status is UP.
[DeviceA-GigabitEthernet1/0/50] quit
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] undo shutdown
[DeviceA-GigabitEthernet1/0/49]
%Jan 18 18:22:46:065 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status is UP.
```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is now up.

Configuration files

- Device A:

```
#
 dldp enable
 dldp work-mode enhance
 dldp unidirectional-shutdown manual
#
interface GigabitEthernet1/0/49
 speed 1000
 duplex full
 dldp enable
#
interface GigabitEthernet1/0/50
 speed 1000
 duplex full
 dldp enable
#
```

- Device B:

  The configuration files on Device B are the same as those on Device A. (Details not shown.)

DNS configuration examples

This chapter provides DNS configuration examples.

DNS services can be static or dynamic. The device checks the static name resolution table for an IP address upon receiving a DNS request. If no IP address is available, it contacts the DNS server for dynamic name resolution. Because dynamic resolution takes more time than static resolution, you can put frequently queried name-to-IP address mappings in the local static name resolution table.

Example: Configuring IPv4 static DNS

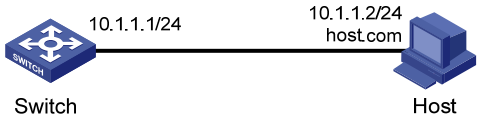
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 61, configure IPv4 static DNS so the switch can access Host by using the domain name **host.com** rather than an IP address.

Figure 61 Network diagram



Configuration procedures

Create a mapping between host name **host.com** and IP address 10.1.1.2.

```
<Switch> system-view
[Switch] ip host host.com 10.1.1.2
```

Verifying the configuration

Use the **ping host.com** command on the switch. The output shows that the switch can use static domain name resolution to resolve domain name **host.com** into IP address 10.1.1.2.

```
<Switch> ping host.com
  PING host.com (10.1.1.2):
  56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=0 ttl=128 time=2 ms
```

```
  Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=128 time=2 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=128 time=2 ms
  Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=128 time=2 ms
  Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=128 time=2 ms

--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/2/2 ms
```

Configuration files

```
#
 ip host host.com 10.1.1.2
#
```

Example: Configuring IPv4 dynamic DNS

Applicable product matrix

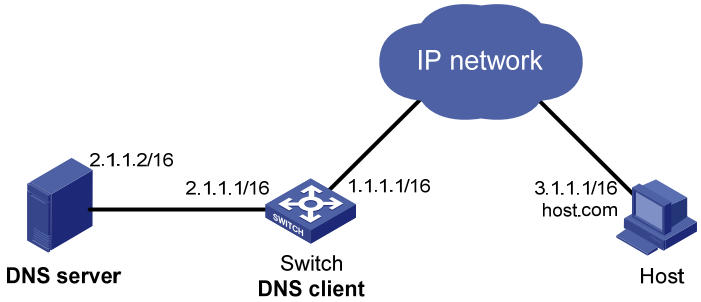
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 62, the switch, the DNS server, and the host can reach each other.

Configure IPv4 dynamic DNS so the switch (DNS client) can use domain name **host.com** to access the host.

Figure 62 Network diagram



Configuration procedures

Configuring the DNS server

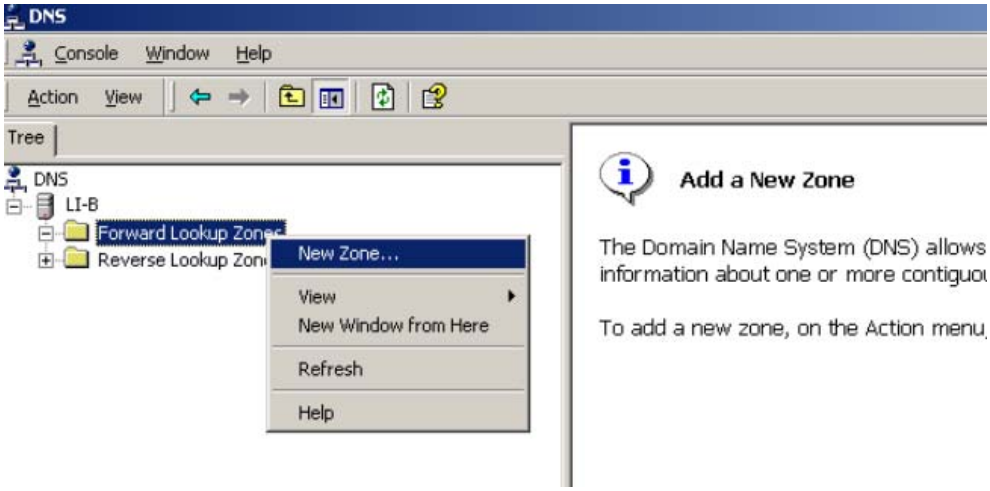
The configuration might vary with DNS servers. The following configuration is performed on a PC running Windows Server 2000.

1. Select **Start** > **Programs** > **Administrative Tools** > **DNS**.

   The DNS server configuration page appears, as shown in Figure 63.

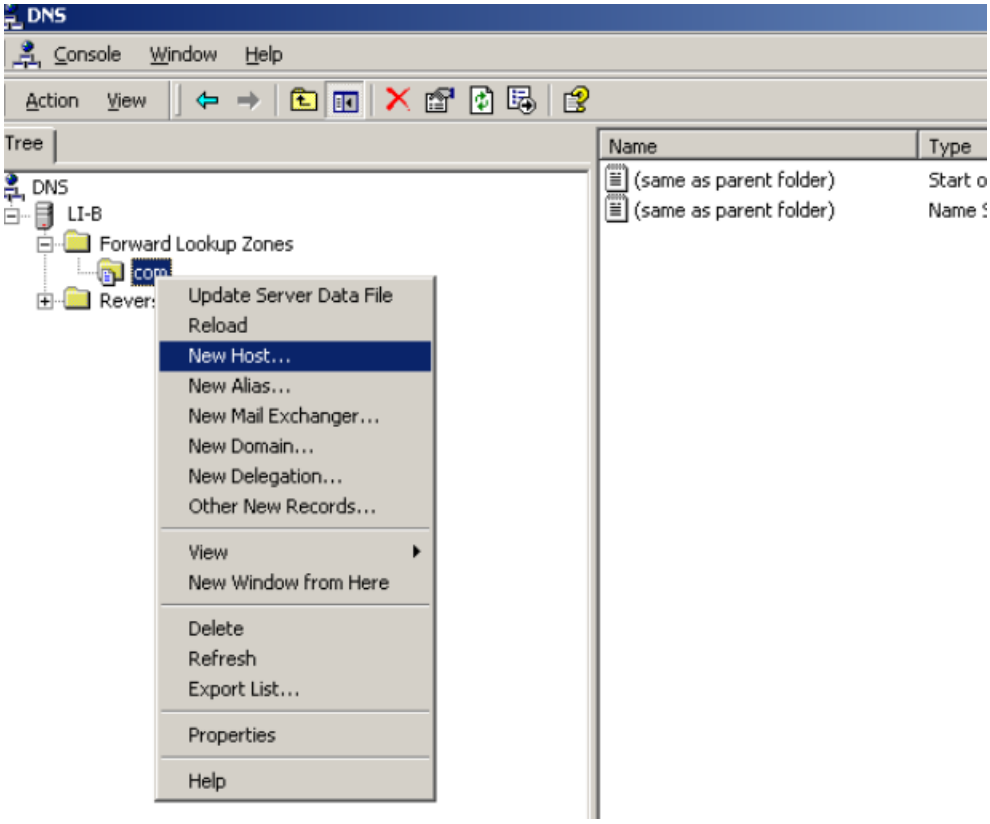
2. Right-click **Forward Lookup Zones**, select **New Zone**, and then follow the wizard to create a new zone named **com**.

Figure 63 Creating a zone



3. On the DNS server configuration page, right-click zone **com** and select **New Host**.

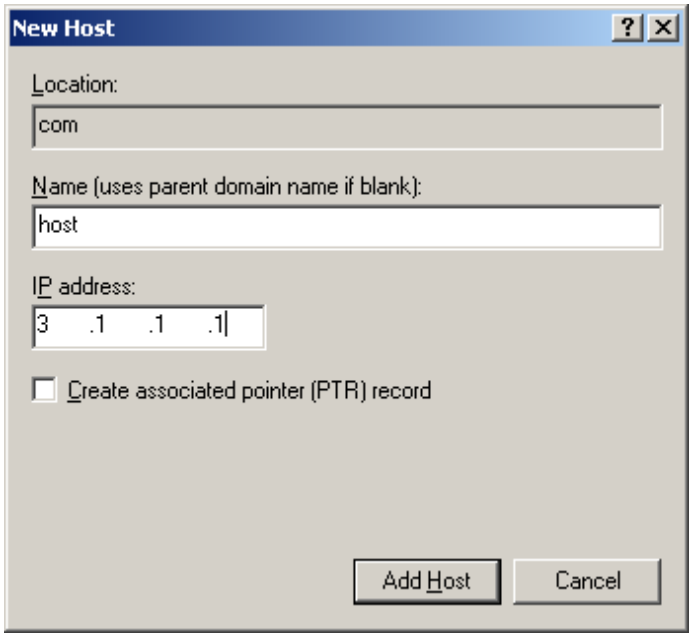
Figure 64 Adding a host



4. On the page that appears, enter host name **host** and IP address **3.1.1.1**.
5. Click **Add Host**.

   The mapping between the IP address and host name is created.

Figure 65 Adding a mapping between domain name and IP address



Configuring the switch

Enable dynamic domain name resolution.

```
<Switch> system-view
[Switch] dns resolve
```

Specify the IP address of the DNS server as 2.1.1.2.

```
[Switch] dns server 2.1.1.2
```

Specify **com** as the name suffix.

```
[Switch] dns domain com
```

Verifying the configuration

Use the **ping host** command on the switch. The output shows that the communication between the switch and the host is correct and that the translated destination IP address is 3.1.1.1.

```
<Switch> ping host
 Trying DNS resolve, press CTRL_C to break
 Trying DNS server (2.1.1.2)
  PING host.com (3.1.1.1):
  56  data bytes, press CTRL_C to break
    Reply from 3.1.1.1: bytes=56 Sequence=0 ttl=126 time=3 ms
    Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms

  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

Configuration files

```
#
 dns resolve
 dns server 2.1.1.2
 dns domain com
#
```

Example: Configuring IPv4 DNS

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

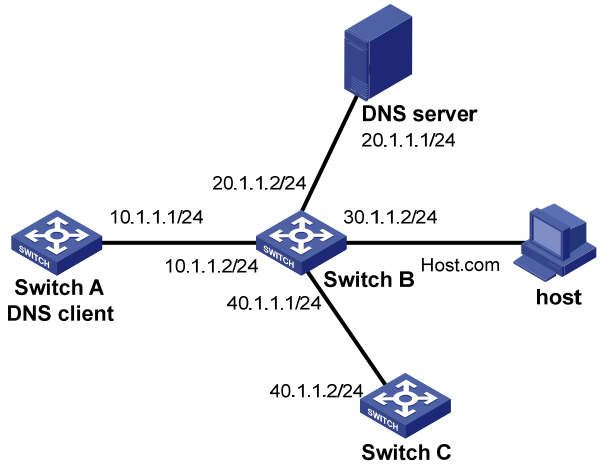
Network requirements

As shown in Figure 66,Switch A, the DNS server, Switch C, and the host can reach each other. Switch A is attempting to access Switch C at a fixed IP address and access the host whose IP address might change.

Configure static and dynamic DNS on Switch A to meet the following requirements:

- Static DNS enables the Switch A to access Switch C by using the domain name of Switch C.
- Dynamic DNS enables Switch A to access the host by using the domain name of the host.

Figure 66 Network diagram



Configuration procedures

Configuring the DNS server

For information about the DNS server configuration, see "Example: Configuring IPv4 dynamic DNS."

Configuring Switch A

Create a mapping between IP address 40.1.1.2 and domain name **SwitchC**.

```
<SwitchA> system-view
[SwitchA] ip host SwitchC 40.1.1.2
```

Enable dynamic domain name resolution.

```
[SwitchA] dns resolve
```

Specify the IP address of the DNS server as 20.1.1.1.

```
[SwitchA] dns server 20.1.1.1
```

Specify **com** as the domain name suffix.

```
[SwitchA] dns domain com
```

Verifying the configuration

Use the **ping SwitchC** command on Switch A. The output shows that Switch A can use static domain name resolution to resolve domain name **SwitchC** into IP address **40.1.1.2**.

```
<SwitchA> ping SwitchC
  PING SwitchC (40.1.1.2):
  56  data bytes, press CTRL_C to break
    Reply from 40.1.1.2: bytes=56 Sequence=1 ttl=126 time=2 ms
    Reply from 40.1.1.2: bytes=56 Sequence=2 ttl=126 time=2 ms
    Reply from 40.1.1.2: bytes=56 Sequence=3 ttl=126 time=2 ms
    Reply from 40.1.1.2: bytes=56 Sequence=4 ttl=126 time=2 ms
    Reply from 40.1.1.2: bytes=56 Sequence=5 ttl=126 time=2 ms

  --- SwitchC ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
```

Use the **ping host** command on Switch A. The output shows that the communication between Switch A and the host is correct and that the translated destination IP address is 3.1.1.1.

```
[SwitchA] ping host
 Trying DNS resolve, press CTRL_C to break
 Trying DNS server (20.1.1.1)
  PING host.com (30.1.1.1):
  56  data bytes, press CTRL_C to break
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms

  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

Configuration files

```
#
 dns resolve
```

```
 dns server 20.1.1.1
 dns domain com
#
ip host host.com 40.1.1.2
#
```

Example: Configuring IPv6 static DNS

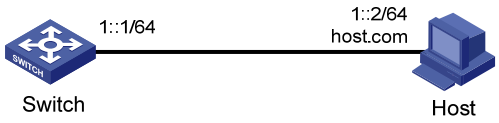
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 67, configure IPv6 static DNS so the switch can access the host by using the domain name **host.com** rather than an IPv6 address.

Figure 67 Network diagram



Configuration procedures

Create a mapping between domain name **host.com** and IPv6 address **1::2**.

```
<Switch> system-view
[Switch] ipv6 host host.com 1::2
```

Enable IPv6.

```
[Switch] ipv6
```

Verifying the configuration

Use the **ping ipv6 host.com** command on the switch. The output shows that the switch can use static domain name resolution to resolve domain name **host.com** into IPv6 address **1::2**.

```
<Switch> ping ipv6 host.com
  PING host.com (1::2):
  56  data bytes, press CTRL_C to break
    Reply from 1::2
    bytes=56 Sequence=0 hop limit=64  time = 3 ms
    Reply from 1::2
```

```
  bytes=56 Sequence=1 hop limit=64  time = 1 ms
  Reply from 1::2
  bytes=56 Sequence=2 hop limit=64  time = 1 ms
  Reply from 1::2
  bytes=56 Sequence=3 hop limit=64  time = 2 ms
  Reply from 1::2
  bytes=56 Sequence=4 hop limit=64  time = 2 ms
--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/3 ms
```

Configuration files

```
#
 ipv6 host host.com 1::2
#
 ipv6
```

Example: Configuring IPv6 dynamic DNS

Applicable product matrix

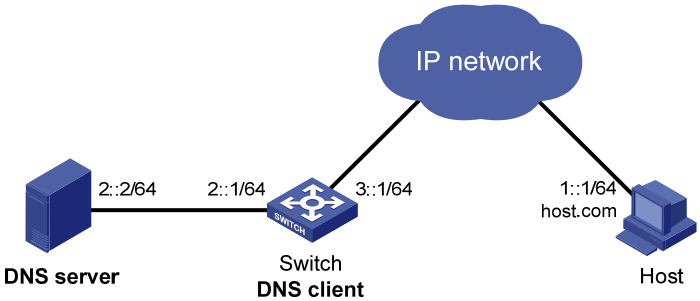
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 68, the switch, the DNS server, and the host can reach each other.

Configure IPv6 dynamic DNS so the switch (DNS client) can use domain name **host.com** to access the host.

Figure 68 Network diagram



Configuration procedures

Configuring the DNS server

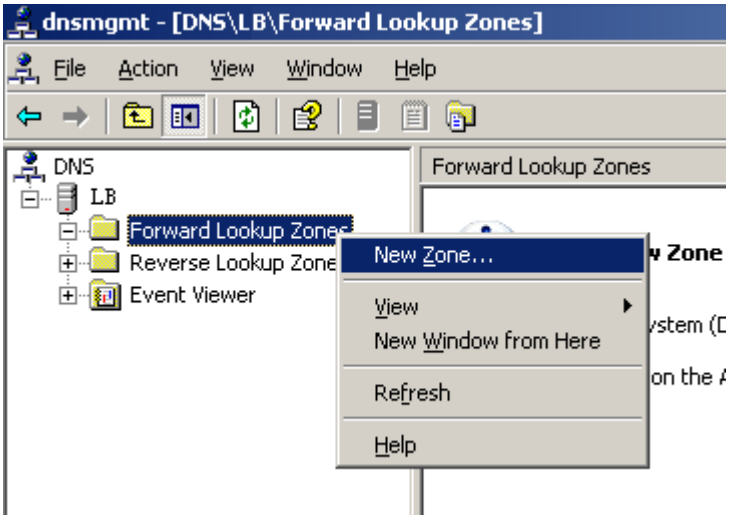
This configuration might vary with DNS servers. The following configuration is performed on a PC running Windows Server 2003.

1. Select **Start** > **Programs** > **Administrative Tools** > **DNS**.

   The DNS server configuration page appears, as shown in Figure 69.

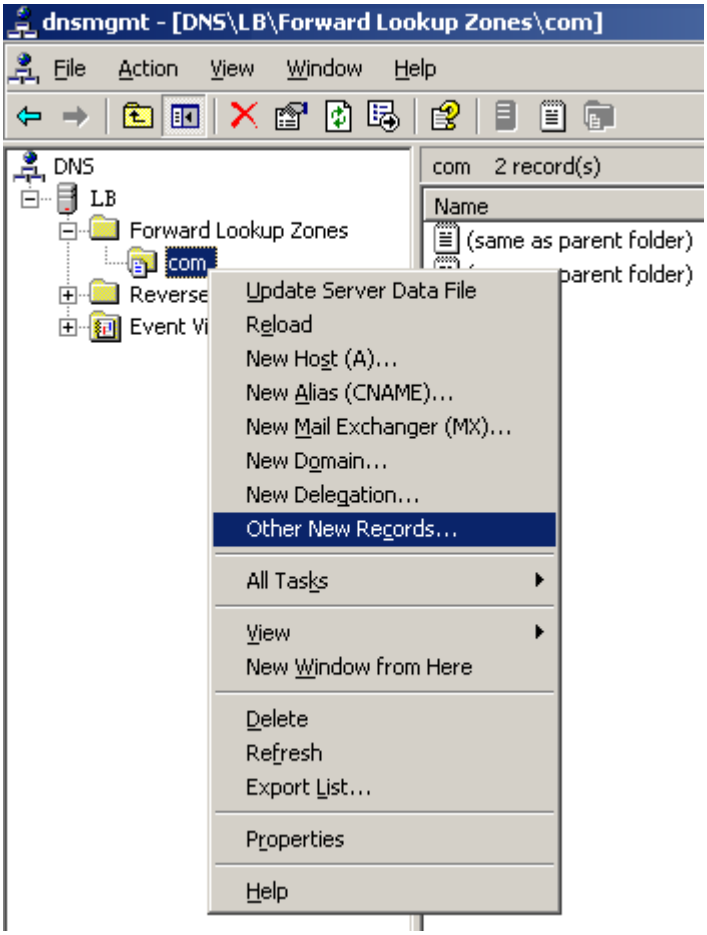
2. Right-click **Forward Lookup Zones**, select **New Zone**, and then follow the wizard to create a new zone named **com**.

Figure 69 Creating a zone



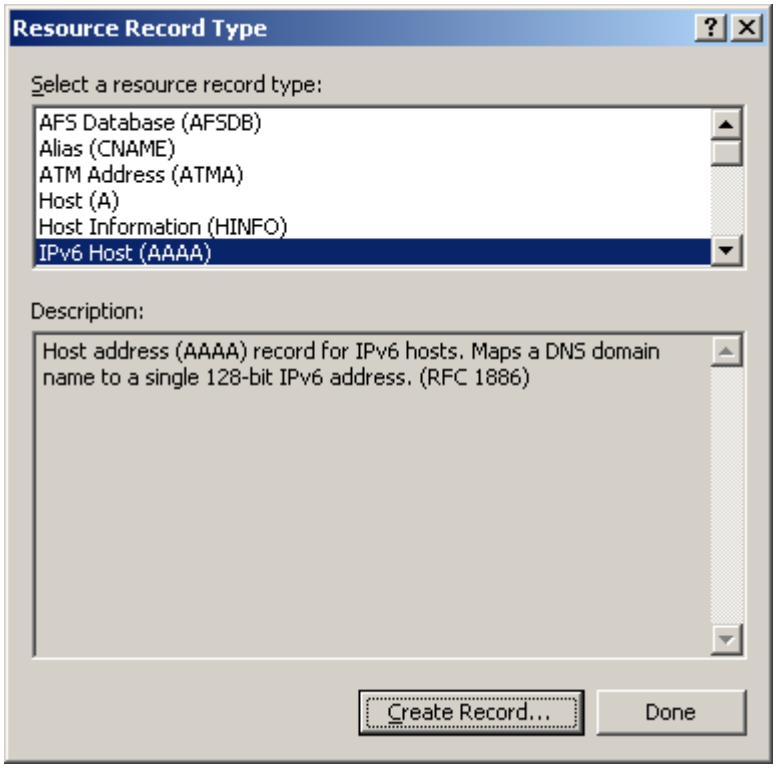
3. On the DNS server configuration page, right-click zone **com**, and select **Other New Records**.

Figure 70 Creating a record



4. On the page that appears, select **IPv6 Host (AAAA)** as the resource record type.

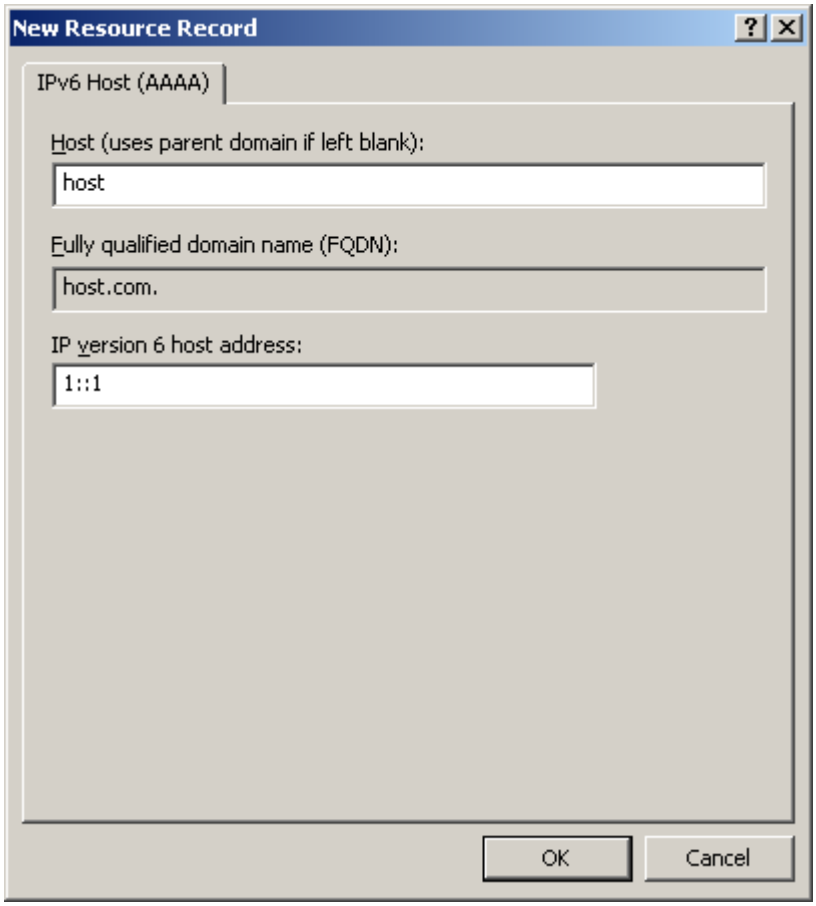
Figure 71 Selecting the resource record type



5. Enter host name **host** and IPv6 address **1::1**.
6. Click **OK**.

   The mapping between the IPv6 address and host name is created.

Figure 72 Adding a mapping between the domain name and IPv6 address



Configuring the Switch

Enable dynamic domain name resolution.

```
<Switch> system-view
[Switch] dns resolve
```

Enable IPv6.

```
[Switch] ipv6
```

Specify the IP address of the DNS server as 2::2.

```
[Switch] dns server ipv6 2::2
```

Specify **com** as the DNS suffix.

```
[Switch] dns domain com
```

Verifying the configuration

Use the **ping ipv6 host** command on the switch. The output shows that that the communication between the switch and the host is correct and that the translated destination IP address is 1::1.

```
<Switch> ping ipv6 host
 Trying DNS resolve, press CTRL_C to break
 Trying DNS server (2::2)
  PING host.com (1::1):
  56  data bytes, press CTRL_C to break
```

```
  Reply from 1::1
  bytes=56 Sequence=0 hop limit=60  time = 2 ms
  Reply from 1::1
  bytes=56 Sequence=1 hop limit=60  time = 1 ms
  Reply from 1::1
  bytes=56 Sequence=2 hop limit=60  time = 1 ms
  Reply from 1::1
  bytes=56 Sequence=3 hop limit=60  time = 1 ms
  Reply from 1::1
  bytes=56 Sequence=4 hop limit=60  time = 1 ms

--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 ms
```

Configuration files

```
#
 dns resolve
 dns server ipv6 2::2
 dns domain com
#
ipv6
#
```

Example: Configuring IPv6 DNS

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

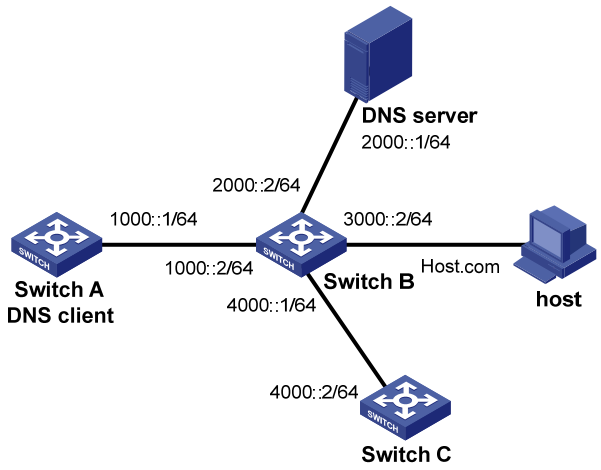
Network requirements

As shown in Figure 73, Switch A, the DNS server, Switch C, and the host can reach each other. Switch A is attempting to access Switch C at a fixed IPv6 address and access the host whose IPv6 address might change.

Configure static and dynamic DNS on Switch A to meet the following requirements:

- Static DNS enables Switch A to access Switch C by using the domain name of Switch C.
- Dynamic DNS enables Switch A to access the host by using the domain name of the host.

Figure 73 Network diagram



Configuration procedures

Configuring the DNS server

For information about the DNS server configuration, see "Example: Configuring IPv6 dynamic DNS."

Configuring Switch A

Create a mapping between IP address 4000::2 and domain name **SwitchC**.

```
<SwitchA> system-view
[SwitchA] ipv6 host SwitchC 4000::2
```

Enable IPv6.

```
[SwitchA] ipv6
```

Enable dynamic domain name resolution.

```
[SwitchA] dns resolve
```

Specify the IP address of the DNS server as 2000::1.

```
[SwitchA] dns server ipv6 2000::1
```

Specify **com** as the domain name suffix.

```
[SwitchA] dns domain com
```

Verifying the configuration

Use the **ping SwitchC** command on Switch A. The output shows that Switch A can use static domain name resolution to resolve domain name **SwitchC** into IP address **4000::2**.

```
<SwitchA> ping ipv6 SwitchC
  PING SwitchC (1::2):
  56  data bytes, press CTRL_C to break
    Reply from 1::2
    bytes=56 Sequence=0 hop limit=63  time = 3 ms
    Reply from 1::2
    bytes=56 Sequence=1 hop limit=63  time = 1 ms
    Reply from 1::2
```

```
    bytes=56 Sequence=2 hop limit=63  time = 1 ms
    Reply from 1::2
    bytes=56 Sequence=3 hop limit=63  time = 2 ms
    Reply from 1::2
    bytes=56 Sequence=4 hop limit=63  time = 2 ms
  --- SwitchC ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

Use the **ping host** command on Switch A. The output shows that the communication between Switch A and the host is correct and that the translated destination IP address is 3000::1.

```
[SwitchA] ping ipv6 host
 Trying DNS resolve, press CTRL_C to break
 Trying DNS server (2000::1)
  PING host.com (3000::1):
  56  data bytes, press CTRL_C to break
    Reply from 3000::1
    bytes=56 Sequence=0 hop limit=63  time = 2 ms
    Reply from 3000::1
    bytes=56 Sequence=1 hop limit=63  time = 1 ms
    Reply from 3000::1
    bytes=56 Sequence=2 hop limit=63  time = 1 ms
    Reply from 3000::1
    bytes=56 Sequence=3 hop limit=63  time = 1 ms
    Reply from 3000::1
    bytes=56 Sequence=4 hop limit=63  time = 1 ms

  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Configuration files

```
#
 dns resolve
 dns server ipv6 2000::1
 dns domain com
#
ipv6 host SwitchC 4000::2
#
ipv6
#
```

Ethernet OAM configuration examples

This document provides Ethernet OAM configuration examples.

Ethernet OAM is a tool that monitors the status of the link between two directly connected switches.

Example: Configuring Ethernet OAM

Applicable product matrix

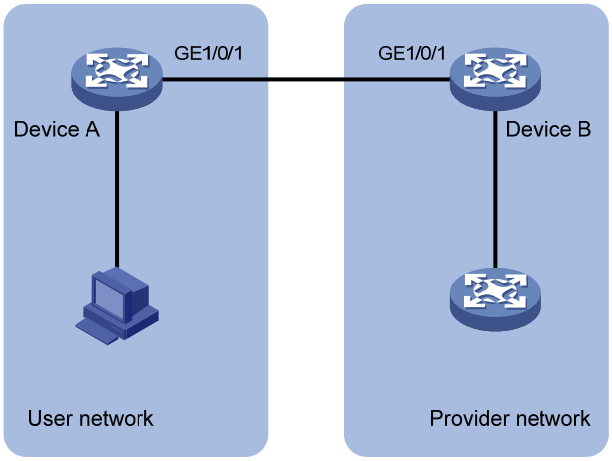
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 74, configure Ethernet OAM on edge switches Device A and Device B to meet the following Service Level Agreement (SLA) requirements:

- Device B of the provider network can initiate Ethernet OAM connection.
- The two switches automatically monitor the link between them.
- The administrator of the provider network can obtain the link status by observing link error event statistics.

Figure 74 Network diagram



Requirement analysis

To facilitate link detection for the provider, configure GigabitEthernet 1/0/1 on Device B to operate in active Ethernet OAM mode.

Configuration procedures

1. Configure Device A:

   # Configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode and enable Ethernet OAM for it.

   ```
   <DeviceA> system-view
   [DeviceA] interface GigabitEthernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] oam mode passive
   [DeviceA-GigabitEthernet1/0/1] oam enable
   [DeviceA-GigabitEthernet1/0/1] quit
   ```

2. Configure Device B:

   # Configure GigabitEthernet 1/0/1 to operate in active Ethernet OAM mode (optional because all ports operate in active Ethernet OAM mode by default) and enable Ethernet OAM for it.

   ```
   <DeviceB> system-view
   [DeviceB] interface GigabitEthernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] oam mode active
   [DeviceB-GigabitEthernet1/0/1] oam enable
   [DeviceB-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Display the Ethernet OAM configuration on Device A.

```
[DeviceA] display oam configuration
Configuration of the link event window/threshold :
--------------------------------------------------------------------------------
Errored-symbol Event period(in seconds)           :     1
Errored-symbol Event threshold                    :     1
Errored-frame Event period(in seconds)            :     1
Errored-frame Event threshold                     :     1
Errored-frame-period Event period(in ms)          :     1000
Errored-frame-period Event threshold              :     1
Errored-frame-seconds Event period(in seconds)    :     60
Errored-frame-seconds Event threshold             :     1

Configuration of the timer :
--------------------------------------------------------------------------------
Hello timer(in ms)                                :     1000
Keepalive timer(in ms)                            :     5000
```

Display Ethernet OAM link event statistics of the remote end on Device B.

```
[DeviceB] display oam link-event remote
Port :GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
--------------------------------------------------------------------
Event Time Stamp          : 5789        Errored FrameWindow   : 10(100ms)
Errored Frame Threshold   : 1           Errored Frame         : 3
Error Running Total       : 35          Event Running Total   : 17
```

The output shows that 35 errors occurred on Device A since the Ethernet OAM connection is established. 17 errors were caused by error frames. The link is instable.

Configuration files

- Device A:

```
#
interface GigabitEthernet1/0/1
 oam mode passive
 oam enable
```

- Device B:

```
#
interface GigabitEthernet1/0/1
 oam enable
```

IGMP configuration examples

This chapter provides examples for configuring IGMP to manage IP multicast group membership.

General configuration restrictions and guidelines

After a Layer 2 multicast protocol is configured on a VLAN, IGMP cannot be enabled on the VLAN interface of this VLAN.

Example: Configuring multicast group filters

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

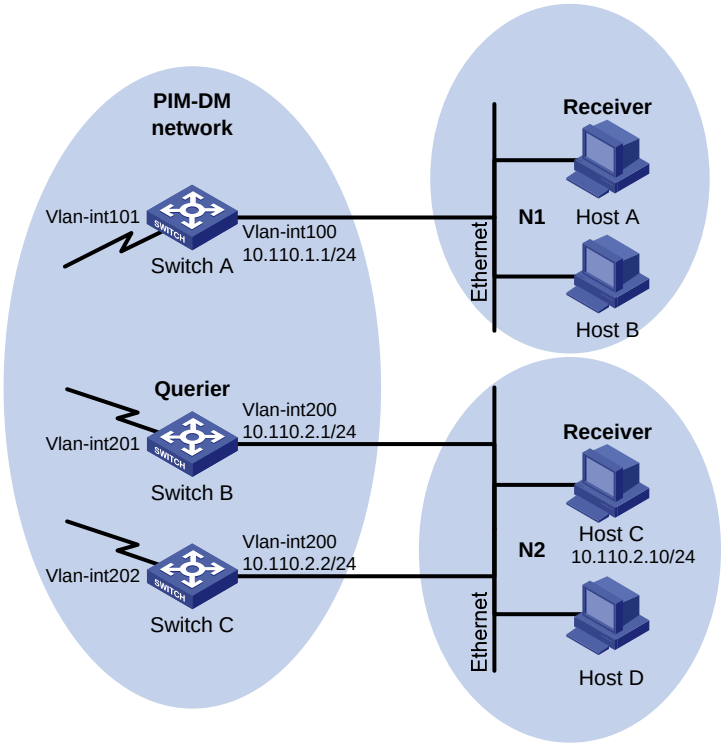
Network requirements

As shown in Figure 75:

- VOD streams are sent to receiver hosts in multicast.
- IGMPv2 runs between Switch A and N1, and between the other two switches and N2.

Configure multicast group filters on Switch B and Switch C so hosts in N2 can join only the multicast group 224.1.1.1. Hosts in N1 can join any multicast group.

Figure 75 Network diagram



Requirements analysis

To limit the IGMP group range that the receivers join, create a basic ACL and specify the multicast group range that matches the **permit** statement in this ACL.

Configuration restrictions and guidelines

When you configure multicast group filters, follow these restrictions and guidelines:

- All Layer 3 switches on the same subnet must run the same version of IGMP.
- To ensure consistent filtering result on the IGMP-enabled switches in N2, you must configure the same multicast group filter on these switches.

Configuration procedures

1. Assign an IP address to each interface in the PIM-DM domain as shown in Figure 75. (Details not shown.)
2. Enable OSPF on all switches on the PIM-DM network to make sure both of the following conditions exist: (Details not shown.)
   - The network layer on the PIM-DM network is interoperable.
   - The switches can dynamically update their routing information.
3. Configure Switch A:

   # Enable IP multicast routing globally

   ```
   <SwitchA> system-view
   ```

```
[SwitchA] multicast routing-enable
```

Enable IGMP and PIM-DM for VLAN interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
```

Enable PIM-DM for VLAN interface 100.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
```

4. Configure Switch B:

Configure an ACL for multicast group filtering.

```
<SwitchB> system-view
[SwitchB] acl number 2001
[SwitchB-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchB-acl-basic-2001] quit
```

Enable IP multicast routing globally.

```
[SwitchB] multicast routing-enable
```

Enable IGMP and PIM-DM for VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
```

Configure a multicast group filter that references ACL 2001 on VLAN-interface 200, so the hosts in N2 can join only the multicast group 224.1.1.1.

```
[SwitchB-Vlan-interface200] igmp group-policy 2001
[SwitchB-Vlan-interface200] quit
```

Enable PIM-DM for VLAN-interface 201.

```
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

5. Configure Switch C:

Configure an ACL for multicast group filtering.

```
<SwitchC> system-view
[SwitchC] acl number 2001
[SwitchC-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchC-acl-basic-2001] quit
```

Enable IP multicast routing globally.

```
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 200
```

Enable IGMP and PIM-DM for VLAN-interface 200.

```
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim dm
```

Configure a multicast group filter that references ACL 2001 on VLAN-interface 200, so the hosts in N2 can join only the multicast group 224.1.1.1.

```
[SwitchC-Vlan-interface200] igmp group-policy 2001
[SwitchC-Vlan-interface200] quit
```

Enable PIM-DM for VLAN-interface 202.

```
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit
```

Verifying the configuration

1. Display information about the IGMP querier in N2:

   # Display information about the IGMP querier on Switch B.

```
[SwitchB] display igmp interface
Interface information of VPN-Instance: public net
 Vlan-interface200(10.110.2.1):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Querier for IGMP: 10.110.2.1 (this router)
  Total 1 IGMP Group reported
```

   # Display information about the IGMP querier on Switch C.

```
[SwitchC] display igmp interface
Interface information of VPN-Instance: public net
 Vlan-interface200(10.110.2.2):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Querier for IGMP: 10.110.2.1
  Total 1 IGMP Group reported
```

   The output shows that Switch B with the smaller IP address has become the IGMP querier on this media-shared subnet.

2. Make Host C in N2 send IGMP membership reports to join multicast groups (224.1.1.1 and 224.1.1.2), and display information about IGMP groups:

   # Display information about IGMP groups on Switch B.

```
[SwitchB] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
 Vlan-interface200(10.110.2.1):
  Total 1 IGMP Groups reported
   Group Address   Last Reporter   Uptime      Expires
   224.1.1.1       10.110.2.10     04:36:03    00:01:23
```

   # Display information about IGMP groups on Switch C.

```
[SwitchC] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
 Vlan-interface200(10.110.2.2):
```

```
  Total 1 IGMP Groups reported
   Group Address   Last Reporter   Uptime      Expires
   224.1.1.1       10.110.2.10     04:21:03    00:01:13
```

The output shows that only information about the multicast group 224.1.1.1 is displayed on Switch B and Switch C, so the configured multicast group filters have taken effect and hosts in N2 can join only the multicast group 224.1.1.1.

Configuration files

- On Switch A:

```
#
 multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 igmp enable
 pim dm
#
interface Vlan-interface101
 pim dm
#
```

- On Switch B:

```
#
 multicast routing-enable
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200 to 201
#
interface Vlan-interface200
 igmp enable
 igmp group-policy 2001
 pim dm
#
interface Vlan-interface201
 pim dm
#
```

- On Switch C:

```
#
 multicast routing-enable
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200 to 202
#
```

```
interface Vlan-interface200
 igmp enable
 igmp group-policy 2001
 pim dm
#
interface Vlan-interface202
 pim dm
#
```

Example: Configuring IGMP SSM mappings

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

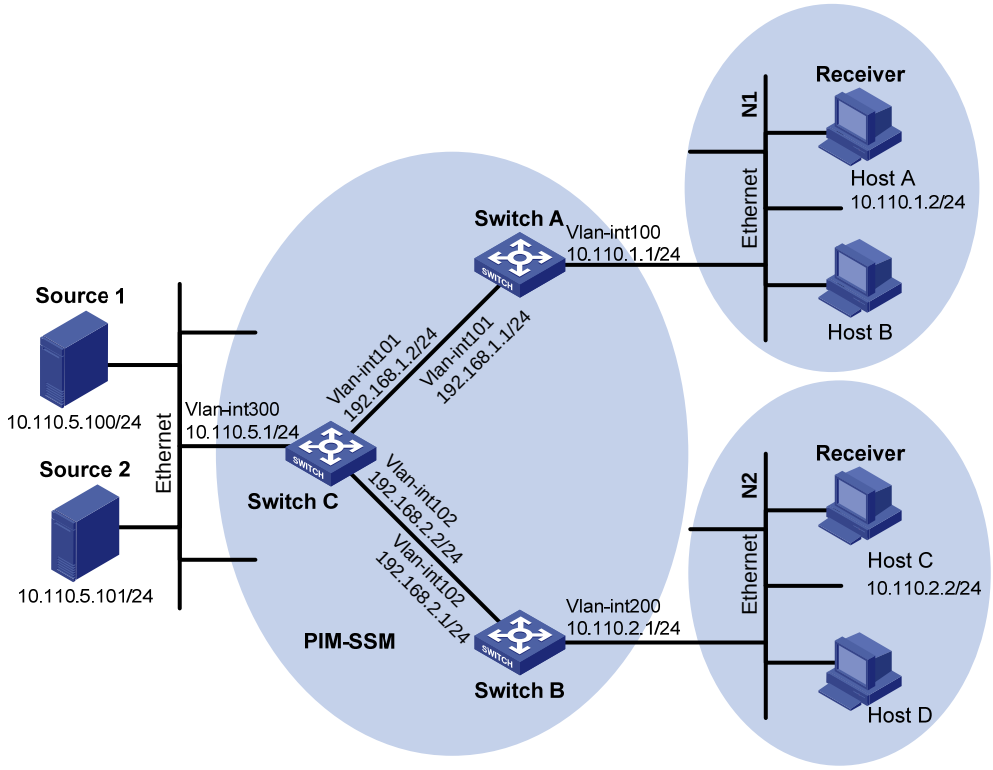
Network requirements

As shown in Figure 76:

- The PIM-SSM network provides services for the multicast groups in the range of 232.1.1.0/24.
- Edge switches of N1 and N2 are running IGMPv3.
- Host A and Host C support IGMPv1 and IGMPv2, but do not support IGMPv3.

Configure IGMP SSM mappings so that Host A and Host C receive multicast data from Source 1 and Source 2, respectively.

Figure 76 Network diagram



Configuration restrictions and guidelines

When you configure IGMP SSM mappings, follow these restrictions and guidelines:

- The IGMP SSM mapping does not process IGMPv3 reports.
- To display information about the multicast groups created based on the configured IGMP SSM mappings, use the **display igmp ssm-mapping group** command.

Configuration procedures

1. Assign an IP address and subnet mask to each interface as shown in Figure 76. (Details not shown.)
2. Enable OSPF on all switches on the PIM-SSM network to make sure both of the following conditions exist: (Details not shown)
   - The network layer on the PIM-SSM network is interoperable.
   - The switches can dynamically update their routing information.
3. Enable IP multicast routing and PIM-SM:

   # On Switch A, enable IP multicast routing globally and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

Enable IP multicast routing and PIM-SM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

4. Enable IGMPv3 on interfaces that connect N1 and N2:

Enable IGMPv3 on VLAN-interface 100 of Switch A. (By default, the IGMP version is 2.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] quit
```

Enable IGMPv3 on Switch B in the same way Switch A is configured. (Details not shown.)

5. Specify the SSM multicast group address range:

On Switch A, specify the SSM multicast group address range as 232.1.1.0/24.

```
[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
[SwitchA-pim] quit
```

Specify the same SSM multicast group address range on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

6. Enable IGMP SSM mapping and configure IGMP SSM mappings:

On Switch A, enable IGMP SSM mapping on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp ssm-mapping enable
[SwitchA-Vlan-interface100] quit
```

Configure an IGMP SSM mapping for the multicast source **Source 1** and multicast groups in the range of 232.1.1.0/24

```
[SwitchA] igmp
[SwitchA-igmp] ssm-mapping 232.1.1.0 24 10.110.5.100
[SwitchA-igmp] quit
```

On Switch B, enable IGMP SSM mapping on VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp ssm-mapping enable
[SwitchB-Vlan-interface200] quit
```

Configure an IGMP SSM mapping for the multicast source Source 2 and multicast groups in the range of 232.1.1.0/24.

```
[SwitchB] igmp
[SwitchB-igmp] ssm-mapping 232.1.1.0 24 10.110.5.101
[SwitchB-igmp] quit
```

Verifying the configuration

1. Make Host A and Host C send the IGMPv2 reports to join the multicast group 232.1.1.1.
2. Display multicast information on Switch A:

Display the IGMP SSM mapping information of the multicast group 232.1.1.1.

```
[SwitchA] display igmp ssm-mapping 232.1.1.1
 VPN-Instance: public net
 Group: 232.1.1.1
 Source list:
        10.110.5.100
```

Display information about the multicast group created based on the configured IGMP SSM mapping.

```
[SwitchA] display igmp ssm-mapping group
 Total 1 IGMP SSM-mapping Group(s).
 Interface group report information of VPN-Instance: public net
 Vlan-interface100(10.110.1.1):
  Total 1 IGMP SSM-mapping Group reported
   Group Address       Last Reporter   Uptime      Expires
   232.1.1.1           10.110.1.2      00:02:04    off
```

Display the PIM routing table.

```
[SwitchA] 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: 00:13:25
     Upstream interface: Vlan-interface101
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
       Total number of downstreams: 1
         1: Vlan-interface100
                 Protocol: igmp, UpTime: 00:13:25, Expires: -
```

3. Display multicast information on Switch B:

Display the IGMP SSM mapping information of the multicast group 232.1.1.1.

```
[SwitchB] display igmp ssm-mapping 232.1.1.1
 VPN-Instance: public net
 Group: 232.1.1.1
 Source list:
        10.110.5.101
```

Display information about the multicast group created based on the configured IGMP SSM mapping.

```
[SwitchB] display igmp ssm-mapping group
 Total 1 IGMP SSM-mapping Group(s).
 Interface group report information of VPN-Instance: public net
 Vlan-interface200(10.110.2.1):
  Total 1 IGMP SSM-mapping Group reported
   Group Address       Last Reporter   Uptime      Expires
   232.1.1.1           10.110.2.2      00:01:15    off
```

Display the PIM routing table.

```
[SwitchB] display pim routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (10.110.5.101, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:12:16
     Upstream interface: Vlan-interface102
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information:
       Total number of downstreams: 1
         1: Vlan-interface200
                 Protocol: igmp, UpTime: 00:05:21, Expires: -
```

The output shows that:

- After an IGMP SSM mapping is configured on Switch A, Switch A translates (0.0.0.0, 232.1.1.1) into (10.110.5.100, 232.1.1.1), so Host A can receive multicast data only from Source 1.
- After an IGMP SSM mapping is configured on Switch B, Switch B translates (0.0.0.0, 232.1.1.1) into (10.110.1.101, 232.1.1.1), so Host C can receive multicast data only from Source 2.

Configuration files

- On Switch A:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
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
#
igmp
```

```
 ssm-mapping 232.1.1.0 24 10.110.5.100
#
pim
 ssm-policy 2000
#
```

- On Switch B:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
 pim sm
#
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
#
igmp
 ssm-mapping 232.1.1.0 24 10.110.5.101
#
pim
 ssm-policy 2000
#
```

- On Switch C:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 101 to 102
#
vlan 300
```

```
#
interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.5.0 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
#
```

IGMP snooping configuration example

This chapter provides examples for configuring IGMP snooping to manage and control multicast group forwarding at Layer 2.

General configuration restrictions and guidelines

IGMP snooping cannot be enabled on a VLAN if the VLAN interface is running a Layer 3 multicast protocol.

Example: Configuring an IGMP snooping multicast group filter

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

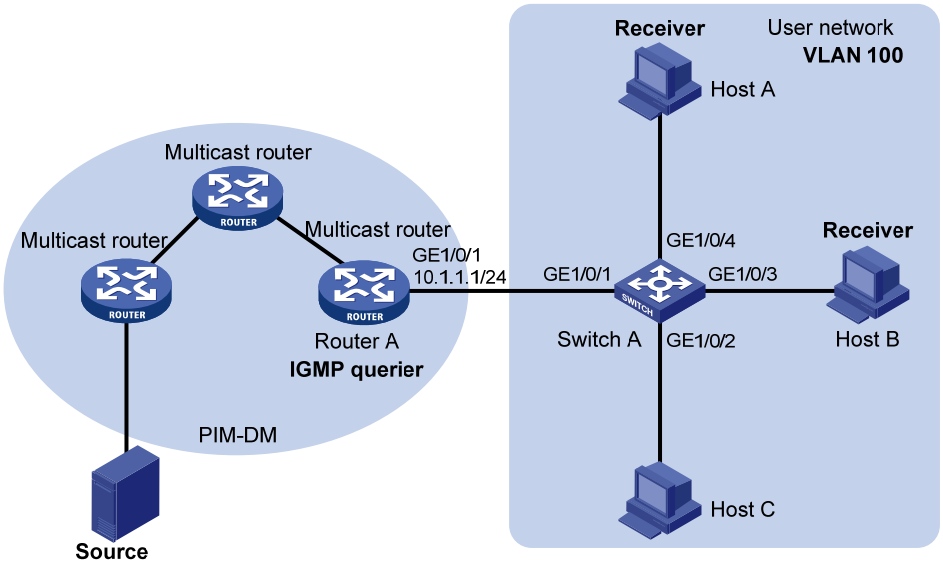
Network requirements

As shown in Figure 77:

- The user network VLAN 100 is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- Users in VLAN 100 want to receive multicast packets from the Source.

Configure an IGMP snooping multicast group filter on Switch A so the receiver hosts in VLAN 100 can receive only the multicast data destined for multicast group 224.1.1.1.

Figure 77 Network diagram



Requirements analysis

To prevent the receiver hosts in VLAN 100 from receiving multicast packets for other multicast groups, enable dropping unknown multicast packets for VLAN 100.

To make sure the IGMP snooping filter controls the multicast groups that hosts can join, create a basic ACL and specify the multicast group range that matches the **permit** statement in the ACL rule.

Configuration restrictions and guidelines

If the ACL for the IGMP snooping multicast group filter does not exist or has no rule, the filter will filter out all multicast groups.

Configuration procedures

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
```

Enable dropping unknown multicast data for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

Create a basic ACL for multicast group filtering.

```
[SwitchA] acl number 2001
```

```
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
```

Configure a multicast group filter that references ACL 2001 for VLAN 100.

```
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

Verifying the configuration

Send IGMP reports from Host A and Host B to join multicast groups 224.1.1.1 and 224.1.1.2, respectively. (Details not shown.)

Display detailed IGMP snooping group information on Switch A.

```
[SwitchA] display igmp-snooping group verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x00000000000000001)
    Router port(s):total 1 port(s).
           GE1/0/1                (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Board
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port(s).
            GE1/0/4                (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port(s).
            GE1/0/4
```

The output shows that only information about the (0.0.0.0, 224.1.1.1) entry is displayed on Switch A. The configured multicast group filter has taken effect.

Configuration files

```
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
```

```
igmp-snooping
 group-policy 2001 vlan 100
#
vlan 100
 igmp-snooping enable
 igmp-snooping drop-unknown
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Configuring IGMP snooping static ports

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

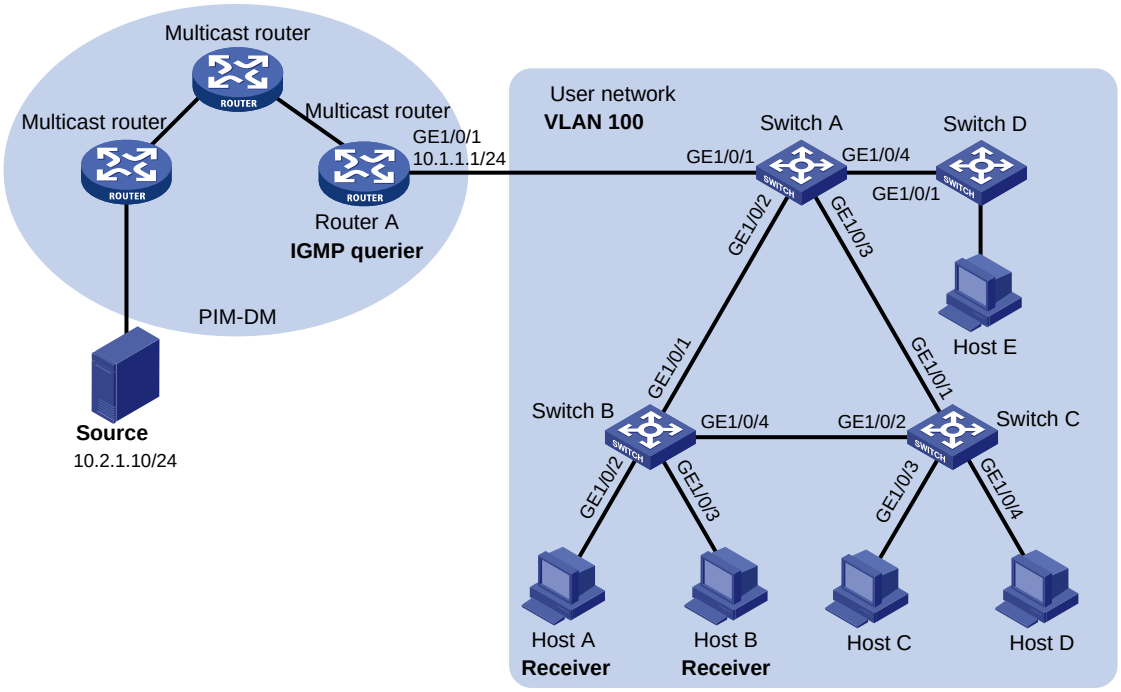
As shown in Figure 78:

- The user network VLAN 100 is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A. Users in VLAN 100 want to receive multicast packets from the Source.
- In the user network, Switch A, Switch B, and Switch C form a ring and are running STP to avoid loops.
- In the user network, dropping unknown multicast packets is enabled on all switches to prevent unknown multicast packets from being flooded.

Configure IGMP snooping static member ports and static router ports to achieve the following goals:

- Host A and Host B receive only multicast packets destined for the multicast group 224.1.1.1.
- Multicast packets can switch from one failed path between Switch A and Switch B to the other path immediately after the new path comes up and becomes stable.

Figure 78 Network diagram



Requirements analysis

To enable the receiver hosts to receive multicast data for a fixed multicast group, configure the ports that are connected to the hosts as IGMP snooping static member ports.

After an STP switchover occurs and the new path becomes stable, at least one IGMP query/response exchange is required before the new path can forward multicast data. For an immediate switchover to the new path, configure all ports that might become multicast data outbound ports as IGMP snooping static router ports on the switches in the ring.

Configuration procedures

Configuring Switch A

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as IGMP snooping static router ports.

```
[SwitchA] interface gigabitethernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch B

Enable IGMP snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as static member ports for the multicast group 224.1.1.1.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
```

Configuring Switch C

Enable IGMP snooping globally.

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

Configure GigabitEthernet 1/0/2 as an IGMP snooping static router port.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Send IGMP reports from Host A and Host B to join multicast group 224.1.1.1.
2. Display IGMP snooping group information.

Display detailed IGMP snooping group information for VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x00000000000000001)
    Router port(s):total 3 port.
            GE1/0/1               (D)
            GE1/0/2               (S)
            GE1/0/3               (S)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Board
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port.
            GE1/0/2              (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port.
            GE1/0/2
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet1/0/3 on Switch A have become IGMP snooping static router ports.

Display detailed IGMP snooping group information for VLAN 100 on Switch B.

```
[SwitchB] display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x00000000000000001)
    Router port(s):total 1 port.
            GE1/0/2              (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
```

```
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Board
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 2 port.
            GE1/0/2                (S)
            GE1/0/3                (S)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 2 port.
            GE1/0/2
            GE1/0/3
```

The output shows that GigabitEthernet1/0/2 and GigabitEthernet 1/0/3 on Switch B have become the static member ports for multicast group 224.1.1.1.

Configuration files

- Switch A:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch B:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
```

```
interface GigabitEthernet1/0/2
 port access vlan 100
 igmp-snooping static group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch C:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Configuring an IGMP snooping querier

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

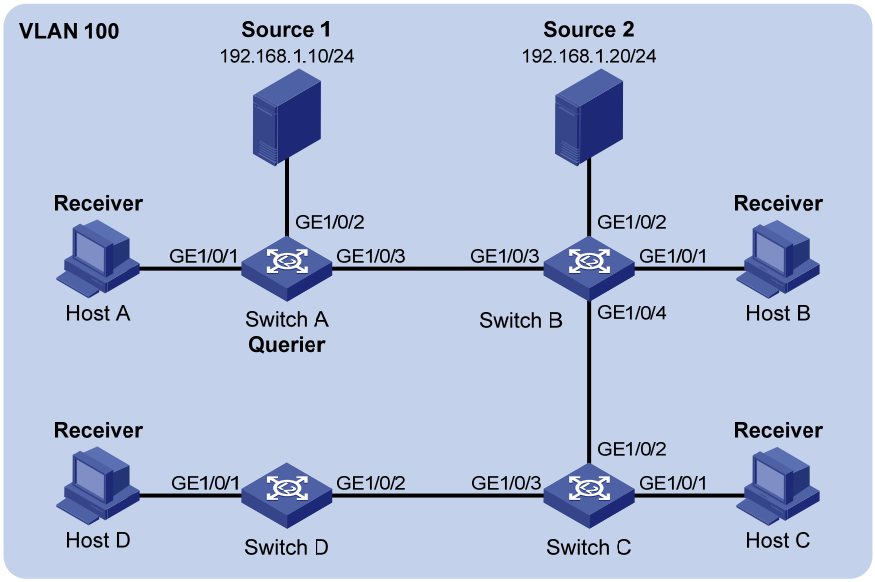
As shown in Figure 79:

- The network is a Layer 2-only network.

- Source 1 and Source 2 send multicast data to the multicast groups 224.1.1.1 and 225.1.1.1, respectively.
- Host A and Host C are receivers of multicast group 224.1.1.1, and Host B and Host D are receivers of multicast group 225.1.1.1.

Configure an IGMP snooping querier so the receiver hosts can receive their expected multicast packets.

Figure 79 Network diagram



Requirements analysis

For all devices between the multicast source and receivers to create Layer 2 multicast forwarding entries, configure the switch that is near to the multicast source as the IGMP snooping querier. In this example, you must configure Switch A as the IGMP snooping querier.

By default, the source IP addresses of the general queries and group-specific queries that the IGMP snooping querier sends are 0.0.0.0. After a switch receives such an IGMP query on a port, it does not enlist the port as a dynamic router port. This might prevent multicast forwarding entries from being correctly created at the data link layer, and eventually cause multicast data unable to be forwarded. To avoid this problem, you must configure a non-all-zero IP address as the source IP address of IGMP queries when a Layer 2 switch acts as the IGMP snooping querier.

Configuration procedures

Configuring Switch A

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable IGMP snooping and IGMP snooping querier for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping querier
```

Specify the source IP address as 192.168.1.1 for the general queries and group-specific queries in VLAN 100.

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit
```

Configuring Switch B

Enable IGMP snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet1/0/1 through GigabitEthernet1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Configuring Switch C and Switch D

Configure Switch C and Switch D in the same way Switch B is configured. (Details not shown.)

Verifying the configuration

Use the **display igmp-snooping statistics** command on a switch to display IGMP packet statistics.

Display statistics for IGMP packets that have been received on Switch B.

```
[SwitchB-vlan100] display igmp-snooping statistics
  Received IGMP general queries:96.
  Received IGMPv1 reports:0.
  Received IGMPv2 reports:105.
  Received IGMP leaves:0.
  Received IGMPv2 specific queries:0.
  Sent     IGMPv2 specific queries:0.
  Received IGMPv3 reports:0.
  Received IGMPv3 reports with right and wrong records:0.
  Received IGMPv3 specific queries:0.
  Received IGMPv3 specific sg queries:0.
  Sent     IGMPv3 specific queries:0.
  Sent     IGMPv3 specific sg queries:0.
  Received error IGMP messages:0.
```

The output shows that the configured IGMP snooping querier has successfully sent out IGMP queries.

Configuration files

- Switch A:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
 igmp-snooping querier
 igmp-snooping general-query source-ip 192.168.1.1
 igmp-snooping special-query source-ip 192.168.1.1
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
```

- Switch B:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

The configuration information on Switch C and Switch D is similar to that on Switch B. (Details not shown.)

Example: Configuring IGMP snooping proxying

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

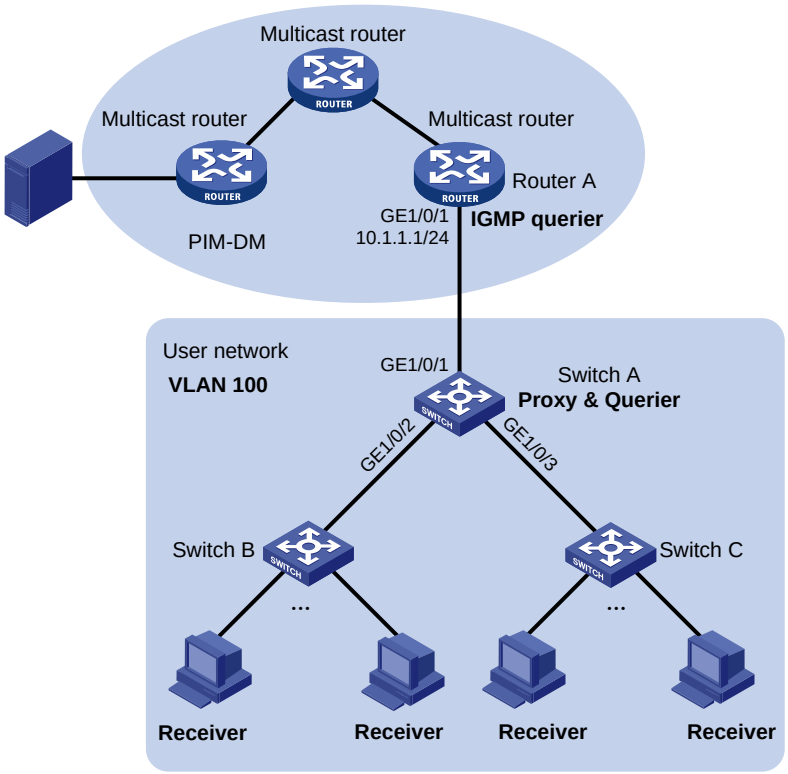
Network requirements

As shown in Figure 80:

- The user network VLAN 100 is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- IGMP snooping is enabled on all switches in VLAN 100.
- Many receivers in VLAN 100 require different VOD data. The receivers frequently join or leave multicast groups, and send large amounts of IGMP report and leave messages to the IGMP querier.

Configure an IGMP snooping proxy to reduce the burden on the IGMP querier.

Figure 80 Network diagram



Requirements analysis

To reduce the number of IGMP report and leave messages received by upstream devices, enable IGMP snooping proxying on the device that is near to the IGMP querier. (Switch A in this example.)

Configuration restrictions and guidelines

Before configuring IGMP snooping proxying, enable IGMP snooping globally and for the relevant VLANs.

Configuration procedures

Configuring Switch A

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable IGMP snooping and IGMP snooping proxying for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping proxying enable
```

Configure the source IP address for IGMP report and leave messages sent by the proxy.

```
[SwitchA-vlan100] igmp-snooping report source-ip 10.1.1.100
[SwitchA-vlan100] igmp-snooping leave source-ip 10.1.1.100
[SwitchA-vlan100] quit
```

Configuring Switch B and Switch C

Create VLAN 100, assign ports that are connected to the receiver hosts to the VLAN, and enable IGMP snooping for the VLAN. (Details not shown.)

Verifying the configuration

1. Send IGMP reports from the receiver hosts in VLAN 100 to join the multicast group 224.1.1.1.
2. Display IGMP group information on Router A.

```
[RouterA] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
 GigabitEthernet1/0/1(10.1.1.1):
   Total 1 IGMP Group reported
    Group Address    Last Reporter    Uptime    Expires
    224.1.1.1        10.1.1.100       00:00:06  00:02:04
```

The output shows that the last reporter address for the multicast group 224.1.1.1 is the configured source IP address for IGMP reports sent by the proxy. The information indicates that Switch A has sent IGMP reports to Router A on behalf of the receiver hosts.

Configuration files

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
 igmp-snooping proxying enable
 igmp-snooping report source-ip 10.1.1.100
 igmp-snooping leave source-ip 10.1.1.100
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
```

IP addressing configuration examples

This chapter provides IP addressing configuration examples.

You can configure primary and secondary IP addresses on an interface of the switch to enable the switch to communicate with hosts in the subnets to which the interface connects.

Example: Configuring IP addressing

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

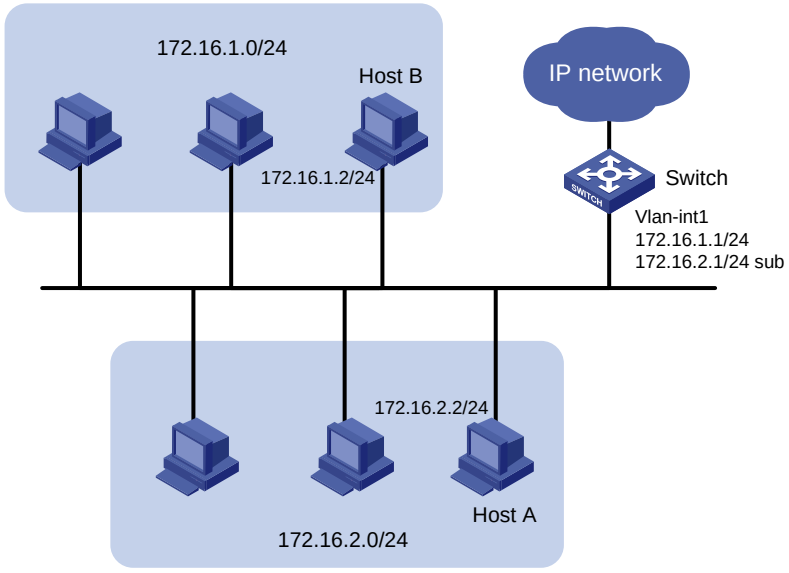
Network requirements

As shown in Figure 81:

- Set the primary IP address of the switch as the gateway address of the hosts on subnet 172.16.1.0/24.
- Set the secondary IP address of the switch as the gateway address of the hosts on subnet 172.16.2.0/24.

The hosts on the LAN can communicate with the external network through the switch.

Figure 81 Network diagram



Configuration procedures

1. Configure the switch:

   # Assign a primary IP address to VLAN-interface 1.

   ```
   <Switch> system-view
   [Switch] interface vlan-interface 1
   [Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
   ```

   # Assign a secondary IP address to VLAN-interface 1.

   ```
   [Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
   [Switch-Vlan-interface1] return
   ```

2. Set the gateway address as follows:
   - 172.16.1.1 on the PCs attached to subnet 172.16.1.0/24.
   - 172.16.2.1 on the PCs attached to subnet 172.16.2.0/24.

Verifying the configuration

Ping a host on subnet 172.16.1.0/24 from the switch to check the connectivity.

```
<Switch> 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=255 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 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
```

The output shows that the switch can communicate with the hosts on subnet 172.16.1.0/24.

Ping a host on subnet 172.16.2.0/24 from the switch to check the connectivity.

```
<Switch> 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=255 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 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
```

The output shows that the switch can communicate with the hosts on subnet 172.16.2.0/24.

Configuration files

```
#
interface Vlan-interface1
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 sub
#
```

IP performance optimization configuration examples

This chapter provides IP performance optimization configuration examples.

Example: Enabling an interface to forward directed broadcasts destined for the directly connected network

Applicable product matrix

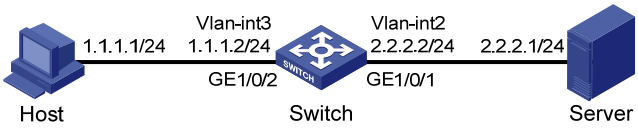
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 82, enable VLAN-interface 2 to forward directed broadcasts destined for the directly connected network.

The server can receive directed broadcasts from the host to IP address 2.2.2.255.

Figure 82 Network diagram



Configuration procedures

1. Configure the switch:

   # Create VLAN 2 and assign GigabitEthernet 1/0/1 to VLAN 2.

   ```
   <Switch> system-view
   [Switch] Vlan 2
   [Switch-vlan2] port GigabitEthernet 1/0/1
   [Switch-Vlan2] quit
   ```

   # Create VLAN 3 and assign GigabitEthernet 1/0/2 to VLAN 3.

   ```
   [Switch] Vlan 3
   [Switch-vlan3] port GigabitEthernet 1/0/2
   ```

```
[Switch–Vlan3] quit
```

Specify IP addresses for VLAN-interface 3 and VLAN-interface 2.

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 1.1.1.2 24
[Switch-Vlan-interface3] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 2.2.2.2 24
```

Enable VLAN-interface 2 to forward directed broadcasts destined for the directly connected network.

```
[Switch-Vlan-interface2] ip forward-broadcast
```

2. Specify the IP address of VLAN-interface 3 as the gateway address of the host.

Verifying the configuration

Ping the subnet-directed broadcast address 2.2.2.255 on the host. The server should be able to receive the ping packets.

Remove the **ip forward-broadcast** configuration on the Vlan-interface, and ping 2.2.2.255 again on the host. The server should not receive the ping packets.

Configuration files

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 2.2.2.2 255.255.255.0
 ip forward-broadcast
#
interface Vlan-interface3
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
```

Example: Enabling sending ICMP destination unreachable packets

You can configure the device to send an ICMP destination unreachable packet when it drops a packet that it cannot forward or deliver. The ICMP destination unreachable packet notifies the source station of the drop event.

Applicable product matrix

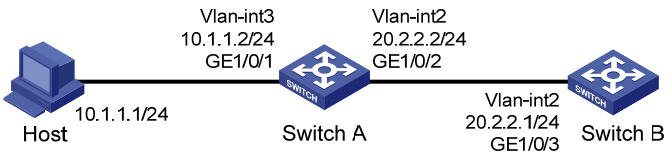
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 83, specify Switch A as the default gateway of the host.

Enable Switch A to send ICMP destination unreachable packets to the host when the IP address of Switch B is incorrectly entered on the host.

Figure 83 Network Diagram



Configuration procedures

1. Configure Switch A:

   # Enable sending ICMP destination unreachable packets.

   ```
   <SwitchA> system-view
   [SwitchA] ip unreachables enable
   ```

   # Create VLAN 3 and assign GigabitEthernet 1/0/1 to VLAN 3.

   ```
   [SwitchA] Vlan 3
   [SwitchA-vlan3] port GigabitEthernet 1/0/1
   [SwitchA-Vlan3] quit
   ```

   # Create VLAN 2 and assign GigabitEthernet 1/0/2 to VLAN 2.

   ```
   [SwitchA] Vlan 2
   [SwitchA-vlan2] port GigabitEthernet 1/0/2
   [SwitchA–Vlan2] quit
   ```

   # Specify IP addresses for VLAN-interface 3 and VLAN-interface 2.

   ```
   [SwitchA] interface vlan-interface 3
   ```

```
[SwitchA-Vlan-interface3] ip address 10.1.1.2 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 20.2.2.2 24
```

2. Configure Switch B:

   # Create VLAN 2 and assign GigabitEthernet 1/0/3 to VLAN 2.

```
<SwitchB> system-view
[SwitchB] Vlan 2
[SwitchB-vlan2] port GigabitEthernet 1/0/3
[SwitchB-Vlan2] quit
```

   # Specify the IP address for VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 20.2.2.1 24
```

   # Configure a static route for Switch B to the host.

```
[SwitchB] ip route-static 10.1.1.0 24 20.2.2.2
```

3. Specify the IP address of VLAN-interface 3 of the switch as the gateway address of the host.

Verifying the configuration

Ping 20.2.2.1 from the host to check the connectivity.

```
C:\ping 20.2.2.1

Pinging 20.2.2.1 with 32 bytes of data:

Reply from 20.2.2.1: bytes=32 time=6ms TTL=254
Reply from 20.2.2.1: bytes=32 time=1ms TTL=254
Reply from 20.2.2.1: bytes=32 time=1ms TTL=254
Reply from 20.2.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 20.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 6ms, Average = 2ms
```

Ping 30.2.2.1 from the host to check the connectivity. The output shows that the address cannot be pinged from the host, and destination unreachable packets are sent back.

```
C:\ping 30.2.2.1

Pinging 30.2.2.1 with 32 bytes of data:

Reply from 10.1.1.2: Destination net unreachable.
Reply from 10.1.1.2: Destination net unreachable.
Reply from 10.1.1.2: Destination net unreachable.
Reply from 10.1.1.2: Destination net unreachable.

Ping statistics for 30.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Configuration files

- Switch A:

```
#
 ip unreachables enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 20.2.2.2 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
 ip route-static 10.1.1.0 255.255.255.0 20.2.2.2
#
```

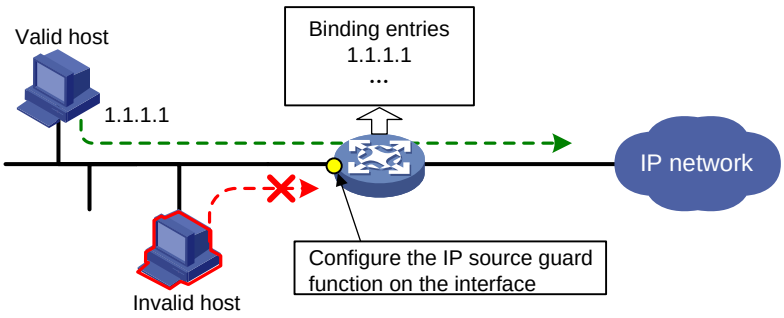
- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 20.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
#
 ip route-static 10.1.1.0 255.255.255.0 20.2.2.2
```

IP source guard configuration examples

This chapter provides IP source guard configuration examples. This security feature filters incoming packets on an interface to prevent spoofing attacks. For example, IP source guard denies access of attackers that use the IP address of a valid host to the network.

Figure 84 Diagram for IP source guard



An IP source guard binding entry can be manually configured or dynamically added.

- **Static IP source guard binding entries**—Applied to scenarios where few hosts exist on a LAN and their IP addresses are manually configured.
- **Dynamic IP source guard binding entries**—Applied to scenarios where DHCP is configured in a LAN with many users.

General configuration restrictions and guidelines

You cannot configure IP source guard on member ports of an aggregate group or service loopback group.

Example: Configuring static IP source guard binding entries

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

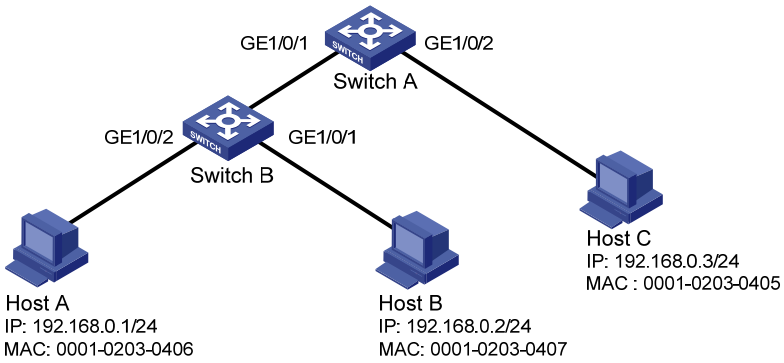
Network requirements

As shown in Figure 85, all hosts use static IP addresses to access the network.

Configure static IPv4 source guard binding entries on Switch A and Switch B to meet the following requirements:

- GigabitEthernet 1/0/1 on Switch A allows only IP packets from Host A to pass.
- GigabitEthernet 1/0/2 on Switch A and interfaces on Switch B allow only IP packets from their own directly connected host to pass.

Figure 85 Network diagram



Configuration procedures

Configuring Switch A

Enable IPv4 source guard on GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Bind the IP address 192.168.0.3 with the MAC address 0001-0203-0405 to form a static IP source guard binding entry on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address
0001-0203-0405
[SwitchA-GigabitEthernet1/0/2] quit
```

Enable IPv4 source guard on GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Bind IP address 192.168.0.1 with the MAC address 0001-0203-0406 to form a static IP source guard binding entry on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[SwitchA-GigabitEthernet1/0/1] quit
```

Configuring Switch B

Enable IPv4 source guard on GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Bind the IP address 192.168.0.1 with the MAC address 0001-0203-0406 to form a static source guard binding entry on GigabitEthernet 1/0/2.

```
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[SwitchB-GigabitEthernet1/0/2] quit
```

Enable IPv4 source guard on GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 address addresses and source MAC address.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Bind the IP address 192.168.0.2 and the MAC address 0001-0203-0407 to form an IP source guard binding entry on GigabitEthernet 1/0/1.

```
[SwitchB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2 mac-address
0001-0203-0407
[SwitchB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display IPv4 source guard binding entries on Switch A.

```
[SwitchA] display ip source binding static
Total entries found: 2
 MAC Address       IP Address       VLAN   Interface           Type
 0001-0203-0406    192.168.0.1      N/A    GE1/0/1             Static
 0001-0203-0405    192.168.0.3      N/A    GE1/0/2             Static
```

Display IPv4 source guard binding entries on Switch B.

```
[SwitchB] display ip source binding static
Total entries found: 2
 MAC Address       IP Address       VLAN   Interface           Type
 0001-0203-0407    192.168.0.2      N/A    GE1/0/1             Static
 0001-0203-0406    192.168.0.1      N/A    GE1/0/2             Static
```

Configuration files

- Switch A:

```
#
interface GigabitEthernet1/0/1
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
 ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/2
 ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
 ip verify source ip-address mac-address
#
```

- Switch B:

```
#
interface GigabitEthernet1/0/1
 ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0407
 ip verify source ip-address mac-address
```

```
#
interface GigabitEthernet1/0/2
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
 ip verify source ip-address mac-address
#
```

Example: Configuring static and dynamic IP source guard

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

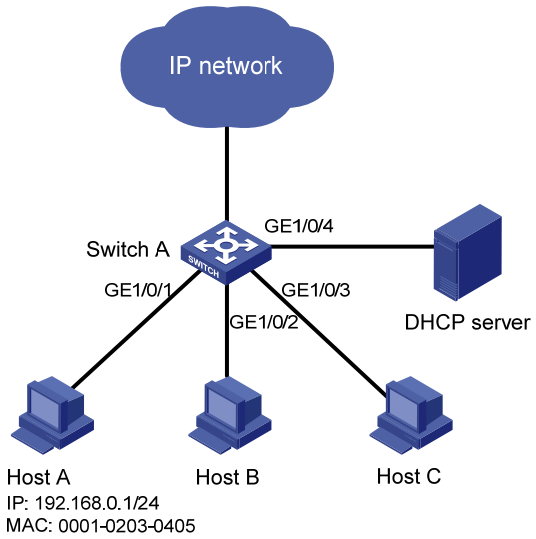
As shown in Figure 86, Host A uses manually configured IP address 192.168.0.1/24. Host B and Host C obtain IP addresses through the DHCP server.

Configure a static IP source guard binding entry on GigabitEthernet 1/0/1 to allow only packets from Host A to pass.

Enable DHCP snooping on the switch so that a DHCP snooping entry can be created for the DHCP client.

Enable IP source guard on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to filter incoming packets based on DHCP snooping entries.

Figure 86 Network diagram



Configuration restrictions and guidelines

You must enable DHCP snooping to make IP source guard dynamic binding entry configuration take effect.

Configuration procedures

Enable IPv4 source guard on GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and MAC addresses.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Bind the source IP address 192.168.0.1 to the source MAC address 0001-0203-0405 to form a static IPv4 source guard binding entry on through GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0405
[SwitchA-GigabitEthernet1/0/1] quit
```

Specify GigabitEthernet 1/0/4 as a trusted port.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/4] quit
```

Enable DHCP snooping.

```
[SwitchA] dhcp-snooping
```

Enable IPv4 source guard on GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and MAC addresses.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[SwitchA-GigabitEthernet1/0/2] quit
```

Enable IPv4 source guard on GigabitEthernet 1/0/3 to filter incoming packets by checking their source IPv4 addresses and MAC addresses.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] ip verify source ip-address mac-address
[SwitchA-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Display IPv4 source guard binding entries.

```
<SwitchA> display ip source binding
Total entries found: 3
 MAC Address       IP Address       VLAN   Interface           Type
 0001-0203-0405    192.168.0.1      N/A    GE1/0/1             Static
 0001-0203-0406    192.168.0.2      1      GE1/0/2             DHCP-SNP
 0001-0203-0407    192.168.0.3      1      GE1/0/3             DHCP-SNP
```

Display DHCP snooping entries.

```
<SwitchA> display dhcp-snooping
```

```
DHCP Snooping is enabled.
The client binding table for all ports.
Type : D--Dynamic , S--Static , R--Recovering
Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
==== =============== ============== ============ ==== ===== =================
D    192.168.0.2     0001-0203-0406 86335        1    N/A   GigabitEthernet1/0/2
D    192.168.0.3     0001-0203-0407 86335        1    N/A   GigabitEthernet1/0/3
```

The output shows that dynamic IP source guard obtains DHCP snooping entries.

Configuration files

```
#
 dhcp-snooping
#
interface GigabitEthernet1/0/1
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0405
 ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/2
 ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/3
 ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/4
 dhcp-snooping trust
#
```

IPv6 basics configuration examples

This chapter provides configuration examples for basic IPv6 settings.

Example: Configuring IPv6 basic settings

Applicable product matrix

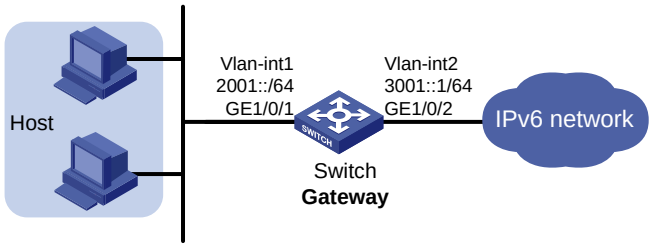
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 87, the switch that serves as a gateway advertises the prefix information in the network segment 2001::/64.

The hosts on this network segment automatically generate IPv6 addresses by using the obtained prefix information, and generate the default routes to the switch.

Figure 87 Network diagram



Configuration procedures

1. Configure the switch:

   # Enable IPv6.

   ```
   <Switch> system-view
   [Switch] ipv6
   ```

   # Specify an EUI-64 IPv6 address for VLAN-interface 1, and allow the interface to advertise RA messages. (By default, no interface advertises RA messages.)

   ```
   [Switch] interface vlan-interface 1
   [Switch-Vlan-interface1] ipv6 address 2001::/64 eui-64
   [Switch-Vlan-interface1] undo ipv6 nd ra halt
   [Switch-Vlan-interface1] quit
   ```

   # Configure a global unicast address for VLAN-interface 2.

```
[Switch] vlan 2
[Switch-vlan2] port GigabitEthernet 1/0/2
[Switch-vlan2] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address 3001::1 64
[Switch-Vlan-interface2] quit
```

2. Configure the hosts:

   Use the **cmd** command on each host to enter the DOS environment, and enable IPv6 for the host.

   ```
   C:\Documents and Settings\aa>ipv6 install
   ```

Verifying the configuration

Display the IPv6 address on a host. The output shows that the host generated an IPv6 address with the prefix 2001::/64, and the gateway is the switch.

Display the IPv6 interface settings on the switch. All the IPv6 addresses configured on the interface are displayed.

```
<Switch> display ipv6 interface
Vlan-interface1 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::223:89FF:FE5F:958C
  Global unicast address(es):
    2001::223:89FF:FE5F:958C, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF5F:958C
    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
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   67
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
```

```
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   26
  OutRequests:                  36
  OutForwDatagrams:             0
  InNoRoutes:                   0
  InTooBigErrors:               0
  OutFragOKs:                   0
  OutFragCreates:               0
  InMcastPkts:                  22
  InMcastNotMembers:            41
  OutMcastPkts:                 21
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::223:89FF:FE5F:958C
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF00:1
    FF02::1:FF5F:958C
    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
IPv6 Packet statistics:
  InReceives:                   8
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   6
  OutRequests:                  8
  OutForwDatagrams:             0
  InNoRoutes:                   0
```

```
InTooBigErrors:                0
OutFragOKs:                    0
OutFragCreates:                0
InMcastPkts:                   3
InMcastNotMembers:             2
OutMcastPkts:                  4
InAddrErrors:                  0
InDiscards:                    0
OutDiscards:                   0
```

Configuration files

```
#
 ipv6
#
vlan 1 to 2
#
interface Vlan-interface1
 undo ipv6 nd ra halt
 ipv6 address 2001::/64 eui-64
#
interface Vlan-interface2
 ipv6 address 3001::1/64
#
interface GigabitEthernet1/0/2
 port access vlan 2
#
```

IPv6 multicast VLAN configuration examples

This document provides IPv6 multicast VLAN configuration examples.

The IPv6 multicast VLAN feature can be implemented by sub-VLAN-based IPv6 multicast VLANs and port-based IPv6 multicast VLANs.

- In a sub-VLAN-based IPv6 multicast VLAN, MLD snooping manages router ports in the IPv6 multicast VLAN and user ports in each sub-VLAN. It is applicable to all networking environments.
- In a port-based IPv6 multicast VLAN, MLD snooping manages the router ports and user ports in the IPv6 multicast VLAN in a centralized way. It is applicable to the networking environment where the device configure with IPv6 multicast VLAN is directly connected to the receivers. It is easy to implement and uses a smaller amount of system resources.

General configuration restrictions and guidelines

Do not configure IPv6 multicast VLAN on a device with IPv6 multicast routing enabled.

Example: Configuring a sub-VLAN-based IPv6 multicast VLAN

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

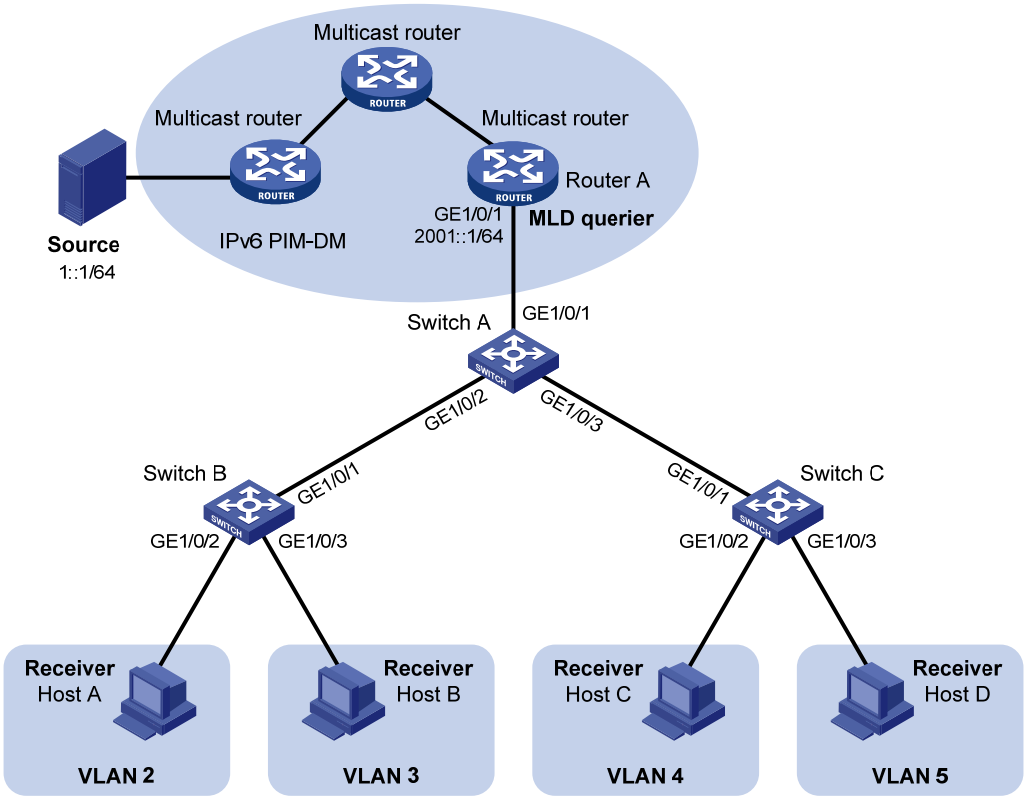
Network requirements

As shown in Figure 88:

- The Layer 2 user network is connected to MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.
- Each user VLAN has a receiver that belongs to the same IPv6 multicast group.

Configure a sub-VLAN-based IPv6 multicast VLAN on Switch A so that Router A can provide multicast services for the hosts through the VLAN.

Figure 88 Network diagram



Configuration restrictions and guidelines

When you configure a sub-VLAN-based IPv6 multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as the IPv6 multicast VLAN must exist.
- A VLAN to be configured as a sub-VLAN must exist and must not be an IPv6 multicast VLAN or a sub-VLAN of any other IPv6 multicast VLANs.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Configure Switch A:

   # Enable MLD snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] mld-snooping
   [SwitchA-mld-snooping] quit
   ```

   # Create VLAN 2 through VLAN 5.

   ```
   [SwitchA] vlan 2 to 5
   ```

   # Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLAN 2 and VLAN 3.

   ```
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] port link-type trunk
   [SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 2 3
   [SwitchA-GigabitEthernet1/0/2] quit
   ```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 4 and VLAN 5.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4 5
[SwitchA-GigabitEthernet1/0/3] quit
```

Create VLAN 1024 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1
```

Enable MLD snooping for VLAN 1024.

```
[SwitchA-vlan1024] mld-snooping enable
[SwitchA-vlan1024] quit
```

Configure VLAN 1024 as an IPv6 multicast VLAN and configure VLAN 2 through VLAN 5 as the sub-VLANs.

```
[SwitchA] multicast-vlan ipv6 1024
[SwitchA-ipv6-mvlan-1024] subvlan 2 to 5
```

3. Configure Switch B:

Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
```

Enable MLD snooping for VLAN 2.

```
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
```

Configure VLAN 3, assign GigabitEthernet 1/0/3 to the VLAN, and enable MLD snooping for the VLAN. (Details not shown.)

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

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2 3
```

4. Configure Switch C in the same way Switch B is configured. (Details not shown.)

Verifying the configuration

Verify that Switch A can receive the reports and forwards the reports to Router A after a host in the VLANs sends MLD reports with the multicast group address FF1E::101,

Display information about the IPv6 multicast VLAN and its sub-VLANs.

```
[SwitchA] display multicast-vlan ipv6
Total 1 IPv6 multicast-vlan(s)

IPv6 multicast vlan 1024
   subvlan list:
    vlan 2-5
   port list:
```

```
    no port
```

Display MLD snooping group information on Switch A.

```
[SwitchA] display mld-snooping group
  Total 5 IP Group(s).
  Total 5 IP Source(s).
  Total 5 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::,FF1E::101):
          Host port(s):total 1 port.
            GE1/0/2                  (D)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            GE1/0/2

  Vlan(id):3.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::, FF1E::101):
          Host port(s):total 1 port.
            GE1/0/2                  (D)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            GE1/0/2

  Vlan(id):4.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::, FF1E::101):
          Host port(s):total 1 port.
```

```
            GE1/0/3                   (D)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            GE1/0/3

  Vlan(id):5.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::, FF1E::101):
          Host port(s):total 1 port.
            GE1/0/3                   (D)
    MAC group(s):
      MAC group address: 3333-0000-0101
          Host port(s):total 1 port.
            GE1/0/3

  Vlan(id):1024.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/1                   (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::, FF1E::101):
          Host port(s):total 0 port.
    MAC group(s):
      MAC group address: 3333-0000-0101
          Host port(s):total 0 port.
```

The output shows that MLD snooping is maintaining router ports in the IPv6 multicast VLAN (VLAN 1024) and maintaining the member ports in their respective sub-VLANs.

Configuration files

```
#
 ipv6
#
 mld-snooping
#
vlan 2 to 5
#
vlan 1024
 mld-snooping enable
```

```
#
multicast-vlan ipv6 1024
 subvlan 2 to 5
#
interface GigabitEthernet1/0/1
 port access vlan 1024
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 3
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 4 to 5
```

Example: Configuring a port-based IPv6 multicast VLAN

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

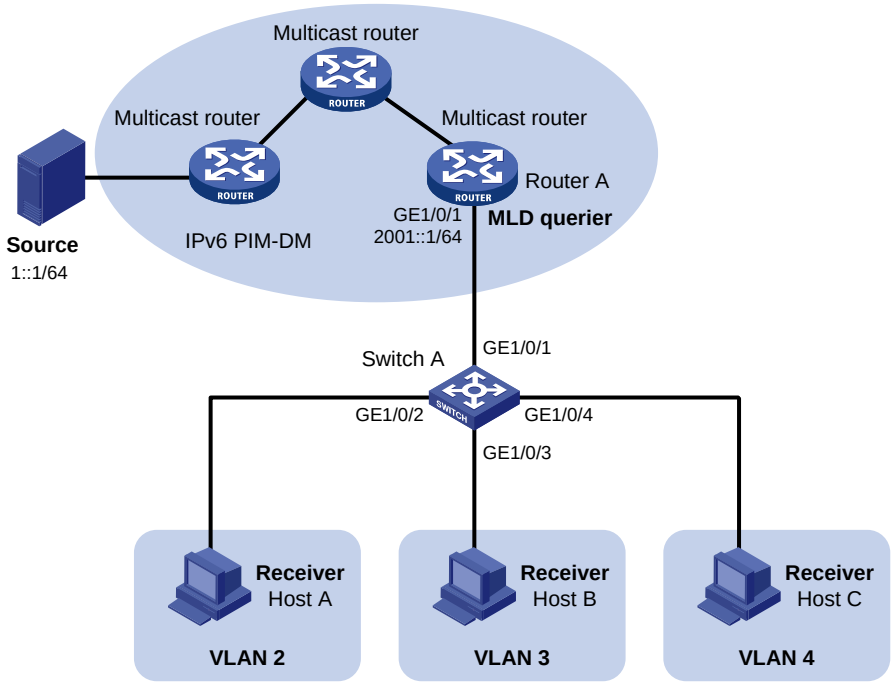
Network requirements

As shown in Figure 89:

- The Layer 2 user network is connected to MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.
- Each user VLAN has a receiver that belong to the same IPv6 multicast group.
- The receivers are directly connected to Switch A.

Configure a port-based IPv6 multicast VLAN on Switch A so that Router A can provide multicast services for the hosts through the VLAN.

Figure 89 Network diagram



Configuration restrictions and guidelines

When you configure a port-based IPv6 multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as the IPv6 multicast VLAN must exist.
- A port can belong to only one IPv6 multicast VLAN.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Configure Switch A:

   # Enable MLD snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] mld-snooping
   [SwitchA-mld-snooping] quit
   ```

   # Create VLAN 1024 and assign GigabitEthernet 1/0/1 to the VLAN.

   ```
   [SwitchA] vlan 1024
   [SwitchA-vlan1024] port gigabitethernet 1/0/1
   ```

   # Enable MLD snooping for VLAN 1024.

   ```
   [SwitchA-vlan1024] mld-snooping enable
   [SwitchA-vlan1024] quit
   ```

   # Create VLAN 2 and enable MLD snooping for the VLAN.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] mld-snooping enable
   [SwitchA-vlan2] quit
   ```

Configure VLAN 3 and VLAN 4 in the same way VLAN 2 is configured. (Details not shown.)

Configure GigabitEthernet 1/0/2 as a hybrid port and configure VLAN 2 as the PVID.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
```

Configure GigabitEthernet 1/0/2 to permit packets from VLAN 2 and VLAN 1024 to pass and untag the packets when forwarding them.

```
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 1024 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a hybrid port and configure VLAN 3 as the PVID. Configure GigabitEthernet 1/0/3 to permit packets from VLAN 3 and VLAN 1024 to pass and untag the packets when forwarding them. (Details not shown.)

Configure GigabitEthernet 1/0/4 as a hybrid port and configure VLAN 4 as the PVID. Configure GigabitEthernet 1/0/4 to permit packets from VLAN 4 and VLAN 1024 to pass and untag the packets when forwarding them. (Details not shown.)

Configure VLAN 1024 as the IPv6 multicast VLAN.

```
[SwitchA] multicast-vlan ipv6 1024
```

Add GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 to the IPv6 multicast VLAN.

```
[SwitchA-ipv6-mvlan-1024] port gigabitethernet 1/0/2 to gigabitethernet 1/0/4
[SwitchA-ipv6-mvlan-1024] quit
```

Verifying the configuration

When hosts in the VLANs send MLD reports with the multicast group address FF1E::101, Switch A should receive the reports and forwards the reports to Router A.

Display information about the IPv6 multicast VLAN.

```
[SwitchA] display multicast-vlan ipv6
 Total 1 IPv6 multicast-vlan(s)

IPv6 multicast vlan 1024
   subvlan list:
    no subvlan
   port list:
    GE1/0/2                  GE1/0/3                  GE1/0/4
```

Display MLD snooping group information.

```
[SwitchA] display mld-snooping group
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):1024.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
```

```
    Router port(s):total 1 port.
            GE1/0/1                 (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::, FF1E::101):
          Host port(s):total 3 port.
            GE1/0/2                 (D)
            GE1/0/3                 (D)
            GE1/0/4                 (D)
    MAC group(s):
      MAC group address: 3333-0000-0101
          Host port(s):total 3 port.
            GE1/0/2
            GE1/0/3
            GE1/0/4
```

The output shows that MLD snooping is maintaining router ports and member ports in the IPv6 multicast VLAN (VLAN 1024).

Configuration files

```
#
 ipv6
#
mld-snooping
#
vlan 2
 mld-snooping enable
#
vlan 3
 mld-snooping enable
#
vlan 4
 mld-snooping enable
#
vlan 1024
 mld-snooping enable
#
multicast-vlan ipv6 1024
#
interface GigabitEthernet1/0/1
 port access vlan 1024
#
interface GigabitEthernet1/0/2
 port link-type hybrid
 port hybrid vlan 1 to 2 1024 untagged
 port hybrid pvid vlan 2
 port multicast-vlan ipv6 1024
#
```

```
interface GigabitEthernet1/0/3
 port link-type hybrid
 port hybrid vlan 1 3 1024 untagged
 port hybrid pvid vlan 3
 port multicast-vlan ipv6 1024
#
interface GigabitEthernet1/0/4
 port link-type hybrid
 port hybrid vlan 1 4 1024 untagged
 port hybrid pvid vlan 4
 port multicast-vlan ipv6 1024
```

IPv6 PIM configuration examples

This chapter provides IPv6 PIM configuration examples.

Based on the implementation mechanism, IPv6 PIM includes the following categories:

- **Protocol Independent Multicast–Dense Mode for IPv6**—IPv6 PIM-DM uses the ASM model and is suitable for small-sized IPv6 networks with densely distributed multicast members.
- **Protocol Independent Multicast–Sparse Mode for IPv6**—IPv6 PIM-SM uses the ASM model and is suitable for large- and medium-sized IPv6 networks with sparsely and widely distributed multicast members. For refined management, IPv6 PIM-SM employs the IPv6 administrative scoping mechanism to provide services for private IPv6 group addresses in specific admin-scoped zones.
- **Protocol Independent Multicast Source-Specific Multicast for IPv6**—IPv6 PIM-SSM provides a solution for IPv6 source-specific multicast.

General configuration restrictions and guidelines

When you configure IPv6 PIM, follow these restrictions and guidelines:

- All the interfaces on a switch must operate in the same IPv6 PIM mode.
- If a VLAN is running a Layer 2 multicast protocol, do not configure Layer 3 multicast protocols on the VLAN interface of this VLAN.

Example: Configuring IPv6 PIM-DM

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 90:

- All the switches are Layer 3 switches, and they run OSPFv3.
- The IPv6 multicast source, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.

Configure IPv6 PIM-DM on each switch, so that multicast data can be sent to receiver hosts in **N1** and **N2**.

Figure 90 Network diagram

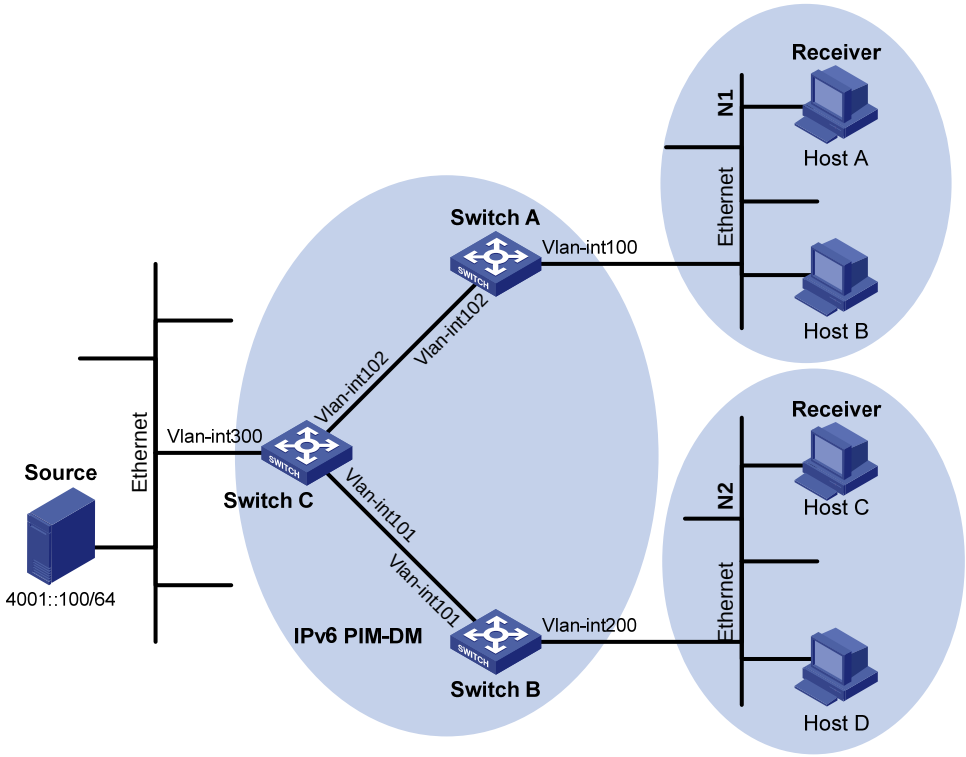


Table 3 shows the interface and IP address assignment, and network topology scheme.

Table 3 Interface and IP address assignment

Device	Interface	IPv6 address
Switch A	VLAN-interface 100	1001::1/64
Switch A	VLAN-interface 102	1002::1/64
Switch B	VLAN-interface 200	2001::1/64
Switch B	VLAN-interface 101	2002::1/64
Switch C	VLAN-interface 300	4001::1/64
Switch C	VLAN-interface 102	1002::2/64
Switch C	VLAN-interface 101	2002::2/64

Configuration restrictions and guidelines

When you configure IPv6 PIM-DM, enable MLD on the edge switches to establish and maintain IPv6 multicast group membership at Layer 3.

Configuration procedures

1. Enable IPv6 forwarding on the switches.
2. Assign an IPv6 address and prefix length to each interface according to Table 3. (Details not shown.)

3. Configure OSPFv3 on the switches in the IPv6 PIM-DM domain. (Details not shown.)
4. Enable IPv6 multicast routing and IPv6 PIM-DM:

   # On Switch A, enable IPv6 multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
```

   # On Switch A, enable IPv6 PIM-DM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 dm
[SwitchA-Vlan-interface102] quit
```

   # On Switch B and Switch C, enable IPv6 multicast routing and IPv6 PIM-DM in the same way Switch A is configured. (Details not shown.)
5. Enable MLD on the interfaces connected to the stub networks **N1** and **N2**:

   # On Switch A, enable MLD (MLDv1 by default) on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] quit
```

   # On Switch B, enable MLD on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

To verify that correct multicast group entries can be created on the switches:

1. Send MLDv1 reports from Host A and Host C to join the IPv6 multicast group **FF0E::101**.
2. Send multicast data from the IPv6 multicast source **4001::100/64** to the IPv6 multicast group.
3. Use the **display pim ipv6 routing-table** command to display IPv6 PIM routing table information on the switches:

   # Display information about the IPv6 PIM routing table on Switch C.

```
[SwitchC] display pim ipv6 routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (4001::100, FF0E::101)
     Protocol: pim-dm, Flag: LOC ACT
     UpTime: 00:02:19
     Upstream interface: Vlan-interface300
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: Vlan-interface101
             Protocol: pim-dm, UpTime: 00:02:19, Expires: never
         2: Vlan-interface102
             Protocol: pim-dm, UpTime: 00:02:19, Expires: never
```

Display information about the IPv6 PIM routing table on Switch A.

```
[SwitchA] display pim ipv6 routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF0E::101)
     Protocol: pim-dm, Flag: WC
     UpTime: 00:01:24
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface100
             Protocol: mld, UpTime: 00:01:20, Expires: never

 (4001::100, FF0E::101)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:01:20
     Upstream interface: Vlan-interface102
         Upstream neighbor: FE80::20F:E2FF:FE67:B323
         RPF prime neighbor: FE80::20F:E2FF:FE67:B323
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface100
             Protocol: pim-dm, UpTime: 00:01:20, Expires: never
```

The output on Switch B is similar to Switch A's output.

The output shows that:

- An SPT is established through traffic flooding. Switches on the SPT paths (Switch A and Switch B) have their (S, G) entries.
- Because Host A sends an MLD report to Switch A to join the IPv6 multicast group, a (*, G) entry is generated on Switch A.

Configuration files

- Switch A:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
vlan 100
#
vlan 102
#
interface Vlan-interface100
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.0
```

```
 mld enable
 pim ipv6 dm
#
interface Vlan-interface102
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 dm
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
```

- Switch B:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
vlan 101
#
vlan 200
#
interface Vlan-interface101
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 dm
#
interface Vlan-interface200
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 pim ipv6 dm
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
```

- Switch C:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
```

```
 ipv6 address 2002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 dm
#
interface Vlan-interface102
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 dm
#
interface Vlan-interface300
 ipv6 address 4001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 dm
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
```

Example: Configuring IPv6 PIM-SM

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 91:

- All the switches are Layer 3 switches, and they run OSPFv3.
- The multicast source, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.

Configure IPv6 PIM-SM on each switch, so that multicast data of the multicast groups in the range of **FF0E::/64** can be sent to receivers in **N1** and **N2**.

Figure 91 Network diagram

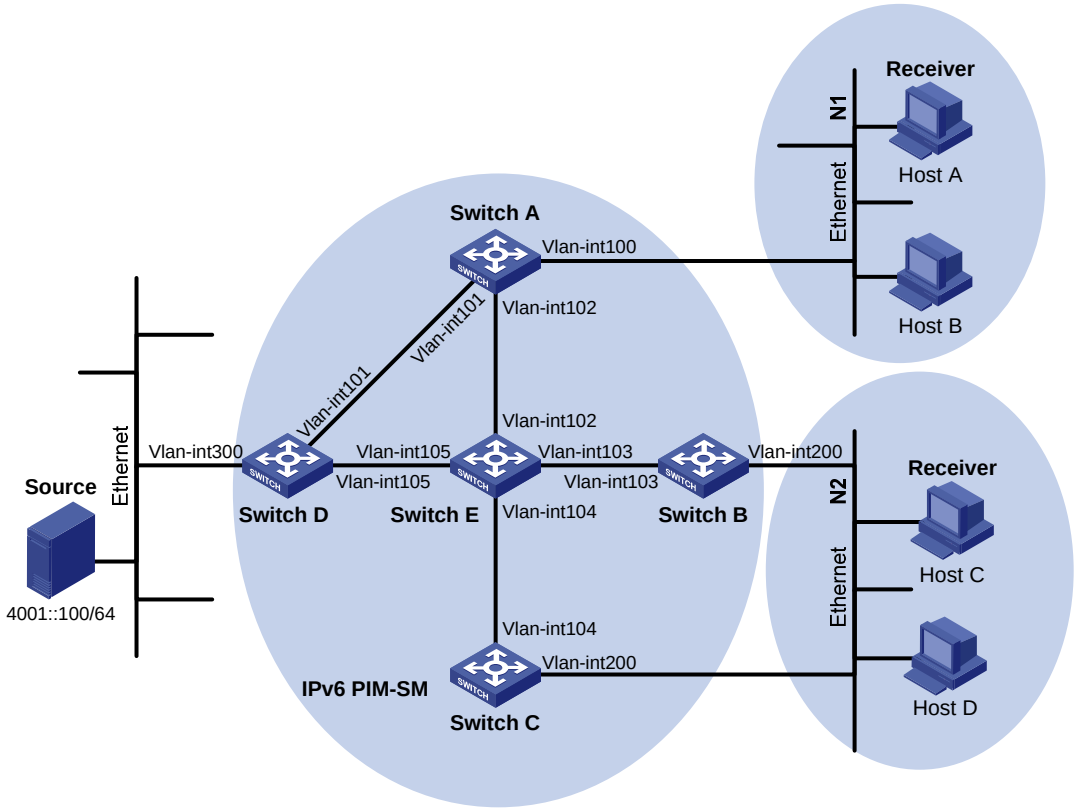


Table 4 shows the interface and IP address assignment, and network topology scheme.

Table 4 Interface and IP address assignment

Device	Interface	IPv6 address
Switch A	VLAN-interface 100	1001::1/64
Switch A	VLAN-interface 101	1002::1/64
Switch A	VLAN-interface 102	1003::1/64
Switch B	VLAN-interface 200	2001::1/64
Switch B	VLAN-interface 103	2002::1/64
Switch C	VLAN-interface 200	2001::2/64
Switch C	VLAN-interface 104	3001::1/64
Switch D	VLAN-interface 300	4001::1/64
Switch D	VLAN-interface 101	1002::2/64
Switch D	VLAN-interface 105	4002::1/64
Switch E	VLAN-interface 104	3001::2/64
Switch E	VLAN-interface 103	2002::2/64
Switch E	VLAN-interface 102	1003::2/64
Switch E	VLAN-interface 105	4002::2/64

Requirements analysis

Because receivers request multicast data of the multicast groups in the range of **FF0E::/64**, you must configure C-RPs to provide services for this group range.

To lessen the burden on a single RP, configure multiple C-RPs on the IPv6 network. For example, configure Switch D and Switch E as C-RPs so they can provide services for different multicast groups through the bootstrap mechanism.

To avoid communication interruption caused by single-point failure of the BSR, configure multiple C-BSRs on the IPv6 network. For example, you can configure a C-BSR on a switch that acts as a C-RP. When the BSR fails, other C-BSRs can elect a new BSR.

Configuration restrictions and guidelines

When you configure IPv6 PIM-SM, follow these restrictions and guidelines:

- If multiple Layer 3 switches are connected to a shared-media network, configure MLD and IPv6 PIM-SM on each Layer 3 switch. When one switch fails, other switches can be used for multicast forwarding, ensuring no interruption to communication.
- HP recommends that you configure C-BSRs and C-RPs on Layer 3 switches on the backbone network.
- If you do not specify the multicast group range to which a C-RP is designated, the C-RP provides services for all multicast groups.

Configuration procedures

1. Enable IPv6 forwarding on the switches.
2. Assign an IPv6 address and prefix length to each interface according to Table 4. (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)
4. Enable IPv6 multicast routing globally and configure IPv6 PIM-SM:

   # On Switch A, enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast ipv6 routing-enable
   ```

   # On Switch A, enable IPv6 PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] pim ipv6 sm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim ipv6 sm
   [SwitchA-Vlan-interface101] quit
   [SwitchA] interface vlan-interface 102
   [SwitchA-Vlan-interface102] pim ipv6 sm
   [SwitchA-Vlan-interface102] quit
   ```

   # On Switch B, Switch C, Switch D, and Switch E, enable IPv6 multicast routing and IPv6 PIM-SM in the same way Switch A is configured. (Details not shown.)
5. Enable MLD on the interfaces connected to the stub networks **N1** and **N2**:

On Switch A, enable MLD (MLDv1 by default) on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] quit
```

On Switch B and Switch C, enable MLD on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

6. Configure C-BSRs and C-RPs:

On Switch D, create an IPv6 ACL to define an IPv6 multicast group range to which the C-RP is designated.

```
<SwitchD> system-view
[SwitchD] acl ipv6 number 2005
[SwitchD-aclv6-basic-2005] rule permit source ff0e:: 64
[SwitchD-aclv6-basic-2005] quit
```

On Switch D, configure VLAN-interface 105 as a C-RP, referencing ACL 2005 to provide services for only the multicast groups in the range of **FF0E::/64**.

```
[SwitchD] pim ipv6
[SwitchD-pim6] c-rp 4002::1 group-policy 2005
```

On Switch D, configure VLAN-interface 105 as a C-BSR, and set its hash mask length and priority to 128 and 10, respectively.

```
[SwitchD-pim6] c-bsr 4002::1 128 10
[SwitchD-pim6] quit
```

On Switch E, create an IPv6 ACL to define an IPv6 multicast group range to which the C-RP is designated.

```
<SwitchE> system-view
[SwitchE] acl ipv6 number 2005
[SwitchE-acl6-basic-2005] rule permit source ff0e:: 64
[SwitchE-acl6-basic-2005] quit
```

On Switch E, configure VLAN-interface 102 as a C-RP, referencing ACL 2005 to provide services for only the multicast groups in the range of **FF0E::/64**.

```
[SwitchE] pim ipv6
[SwitchE-pim6] c-rp 1003::2 group-policy 2005
```

On Switch E, configure VLAN-interface 102 as a C-BSR, and set its hash mask length and priority to 128 and 20, respectively.

```
[SwitchE-pim6] c-bsr 1003::2 128 20
[SwitchE-pim6] quit
```

Verifying the configuration

1. Verify that the MLD querier and the DR are correctly elected on the shared-media network **N2**:

Display MLD querier information on Switch B.

```
[SwitchB] display mld interface
Interface information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958B):
   MLD is enabled
   Current MLD version is 1
   Value of query interval for MLD(in seconds): 125
```

```
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Querier for MLD: FE80::223:89FF:FE5F:958B (this router)
  Total 1 MLD Group reported
```

Display MLD querier information on Switch C.

```
[SwitchC] display mld interface
Interface information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958C):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Querier for MLD: FE80::223:89FF:FE5F:958B
  Total 1 MLD Group reported
```

The output shows that Switch B is elected the MLD querier. The switch with a lower IPv6 link-local address wins the MLD querier election.

Display IPv6 PIM information on Switch B

```
[SwitchB] display pim ipv6 interface
 VPN-Instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan103             1      30         1          FE80::223:89FF:
                                                  FE5F:958E
 Vlan200             1      30         1          FE80::223:89FF:
                                                  FE5F:958C
```

Display IPv6 PIM information on Switch C.

```
[SwitchC] display pim ipv6 interface
 VPN-Instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan104             1      30         1          FE80::223:89FF:
                                                  FE5F:958E
 Vlan200             1      30         1          FE80::223:89FF:
                                                  FE5F:958C (local)
```

The output shows that Switch C is elected the DR. The switch that has a higher IPv6 link-local address wins the DR election if the two switches have the same DR priority. The DR priority is identified by the DR priority field in hello packets.

2. Verify that correct IPv6 multicast group entries can be created on the switches:
   a. Send an MLDv1 report from Host A to join the IPv6 multicast group **FF0E::100**.
   b. Send multicast data from the multicast source **4001::100/64** to the IPv6 multicast group.
   c. Use the **display pim ipv6 routing-table** command to display IPv6 PIM routing table information on the switches:

      # Display information about the IPv6 PIM routing table on Switch A.

      ```
      [SwitchA] display pim ipv6 routing-table
       VPN-Instance: public net
       Total 1 (*, G) entry; 1 (S, G) entry
      ```

```
 (*, FF0E::100)
     RP: 1003::2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:03:45
     Upstream interface: Vlan-interface102
         Upstream neighbor: FE80::223:89FF:FE5F:958E
         RPF prime neighbor: FE80::223:89FF:FE5F:958E
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface100
             Protocol: mld, UpTime: 00:02:15, Expires: 00:03:06

 (4001::100, FF0E::100)
     RP: 1003::2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:02:15
     Upstream interface: Vlan-interface101
         Upstream neighbor: FE80::223:89FF:FE5F:958D
         RPF prime neighbor: FE80::223:89FF:FE5F:958D
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface100
             Protocol: pim-sm, UpTime: 00:02:15, Expires: 00:03:06
```

The output on Switch B and Switch C is similar to Switch A's output.

Display information about the IPv6 PIM routing table on Switch D.

```
[SwitchD] display pim ipv6 routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (4001::100, FF0E::100)
     RP: 1003::2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 00:14:44
     Upstream interface: Vlan-interface300
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface101
             Protocol: mld, UpTime: 00:14:44, Expires: 00:02:26
```

Display information about the IPv6 PIM routing table on Switch E.

```
[SwitchE] display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF0E::100)
     RP: 1003::2 (local)
     Protocol: pim-sm, Flag: WC
```

```
    UpTime: 00:16:56
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlan-interface102
            Protocol: pim-sm, UpTime: 00:16:56, Expires: 00:02:34

 (4001::100, FF0E::100)
     RP: 1003::2 (local)
     Protocol: pim-sm, Flag: RPT SPT ACT
     UpTime: 00:25:32
     Upstream interface: Vlan-interface105
         Upstream neighbor: FE80::223:89FF:FE5F:958D
         RPF prime neighbor: FE80::223:89FF:FE5F:958D
     Downstream interface(s) information: None
```

The output shows the following:

- The RP for the multicast group **FF0E::100** is Switch E as a result of hash calculation.
- An SPT has been built between the source-side DR (Switch D) and the RP (Switch E).
- An RPT has been built between the receiver-side DR (Switch A) and the RP (Switch E), and Switch A and Switch E have created (*, G) entries.
- After receiving IPv6 multicast data, the receiver-side DR (Switch A) immediately switches from the RPT to the SPT. A new SPT is built between the receiver-side DR (Switch A) and the source-side DR (Switch D). The switches (Switch A and Switch D) on the new SPT path have their (S, G) entries.

Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 pim ipv6 sm
#
interface Vlan-interface101
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
```

```
#
interface Vlan-interface102
 ipv6 address 1003::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
```

- Switch B:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 103
#
vlan 200
#
interface Vlan-interface103
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface200
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 pim ipv6 sm
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
```

- Switch C:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 104
#
vlan 200
#
interface Vlan-interface104
 ipv6 address 3001::1/64
 ospfv3 1 area 0.0.0.0
```

```
 pim ipv6 sm
#
interface Vlan-interface200
 ipv6 address 2001::2/64
 ospfv3 1 area 0.0.0.0
 mld enable
 pim ipv6 sm
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
```

- Switch D:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2005
 rule 0 permit source FF0E::/64
#
vlan 101
#
vlan 105
#
vlan 300
#
interface Vlan-interface101
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface105
 ipv6 address 4002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface300
 ipv6 address 4001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
pim ipv6
 c-bsr hash-length 128
 c-bsr priority 10
 c-bsr 4002::1
 c-rp 4002::1 group-policy 2005
#
```

```
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
#
```

- Switch E:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2005
 rule 0 permit source FF0E::/64
#
vlan 102 to 104
#
vlan 105
#
interface Vlan-interface102
 ipv6 address 1003::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface103
 ipv6 address 2002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface104
 ipv6 address 3001::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface105
 ipv6 address 4002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
pim ipv6
c-bsr hash-length 128
 c-bsr priority 20
 c-bsr 1003::2
 c-rp 1003::2 group-policy 2005
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
#
```

Example: Configuring IPv6 PIM-SM admin-scoped zones

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 92:

- All switches are Layer 3 switches, and they run OSPFv3.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.

Use the IPv6 PIM-SM administrative scoping mechanism to achieve the following purposes:

- Divide the whole network into admin-scoped zone 1, admin-scoped zone 2, and the global-scoped zone.
- Each admin-scoped zone provides services for IPv6 multicast groups with the scope field of **4**. Source 1 in admin-scoped zone 1 and Source 2 in admin-scoped zone 2 send multicast data only to these IPv6 multicast groups. Receivers in each admin-scoped zone can request multicast data only within the local zone.
- Source 3 in the global-scoped zone sends multicast data to all multicast groups with the scope field value of **14**. All receivers on the network can request multicast data of these multicast groups.

Figure 92 Network diagram

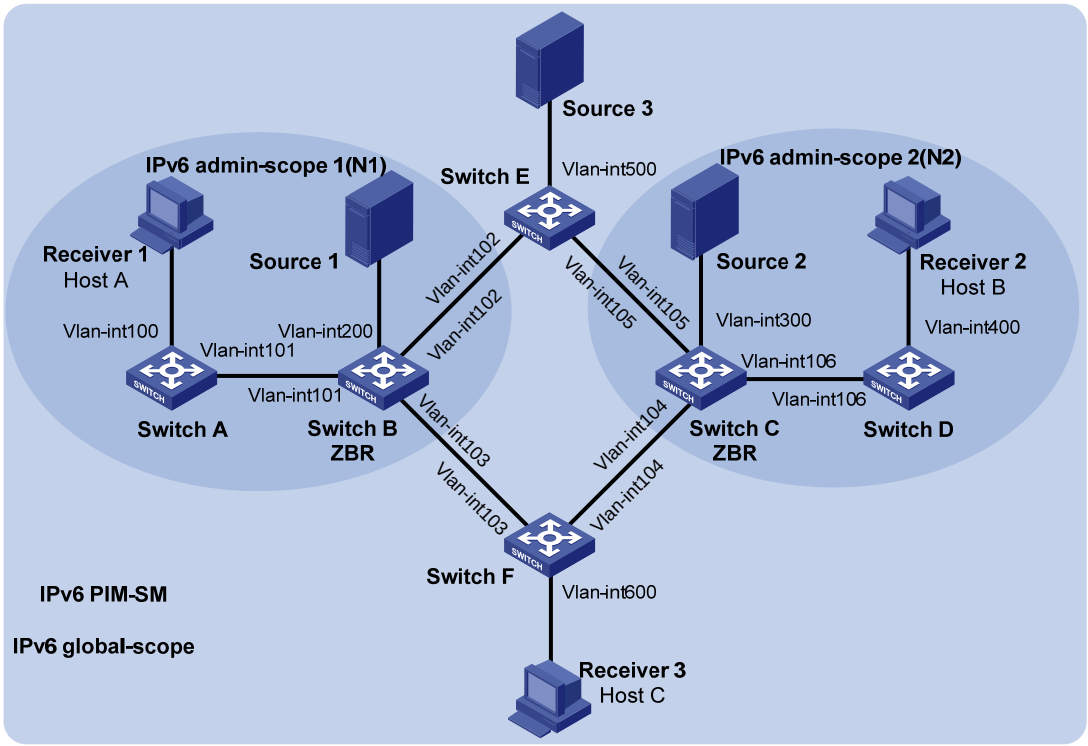


Table 5 IP address assignment

Device	Interface	IPv6 address	Device	Interface	IPv6 address
Switch A	VLAN-interface 100	1001::1/64	Switch D	VLAN-interface 106	1007::2/64
Switch A	VLAN-interface 101	1002::1/64	Switch E	VLAN-interface 500	5001::1/64
Switch B	VLAN-interface 200	2001::1/64	Switch E	VLAN-interface 102	1003::2/64
Switch B	VLAN-interface 101	1002::2/64	Switch E	VLAN-interface 105	1006::2/64
Switch B	VLAN-interface 102	1003::1/64	Switch F	VLAN-interface 600	6001::1/64
Switch B	VLAN-interface 103	1004::1/64	Switch F	VLAN-interface 103	1004::2/64
Switch C	VLAN-interface 300	3001::1/64	Switch F	VLAN-interface 104	1005::2/64
Switch C	VLAN-interface 104	1005::1/64	Source 1	N/A	2001::100/64
Switch C	VLAN-interface 105	1006::1/64	Source 2	N/A	3001::100/64
Switch C	VLAN-interface 106	1007::1/64	Source 3	N/A	5001::100/64
Switch D	VLAN-interface 400	4001::1/64			

Requirements analysis

Configure the boundaries of each admin-scoped zone on the interfaces through which it connects other zones based on the following considerations:

- The division of admin-scoped zones.
- The IPv6 multicast group range to which each zone is designated.

To use the admin-scoped zones and the global-scoped zone to provide services for specific IPv6 multicast groups, configure C-BSRs and C-RPs in each zone as follows:

- The C-BSRs and C-RPs in each admin-scoped zone provide services for the IPv6 multicast groups to which the admin-scoped zone is designated.
- The C-BSRs and C-RPs in the global-scoped zone provide services for all IPv6 multicast groups except multicast groups to which admin-scoped zones are designated.

Configuration restrictions and guidelines

When you configure IPv6 PIM-SM admin-scoped zones, follow these restrictions and guidelines:

- To establish and maintain IPv6 multicast group membership at Layer 3, enable MLD on the interfaces of switches that are directly connected to receiver hosts.
- Before you configure IPv6 admin-scoped zones, enable IPv6 administrative scoping on all Layer 3 switches in the IPv6 PIM-SM domain.

Configuration procedures

1. Enable IPv6 forwarding on the switches.
2. Assign an IPv6 address and prefix length to each interface according to Table 5. (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)
4. Enable IPv6 multicast routing, IPv6 administrative scoping, and IPv6 PIM-SM:

   # On Switch A, enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast ipv6 routing-enable
   ```

   # On Switch A, enable IPv6 administrative scoping globally.

   ```
   [SwitchA] pim ipv6
   [SwitchA-pim6] c-bsr admin-scope
   [SwitchA-pim6] quit
   ```

   # On Switch A, enable IPv6 PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] pim ipv6 sm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim ipv6 sm
   [SwitchA-Vlan-interface101] quit
   ```

   # On Switch B, Switch C, Switch D, Switch E, and Switch F, enable IPv6 multicast routing, IPv6 administrative scoping, and IPv6 PIM-SM in the same way Switch A is configured. (Details not shown.)
5. Enable MLD on the interfaces connected to the receiver hosts:

   # On Switch A, enable MLD on VLAN-interface 100.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] mld enable
   [SwitchA-Vlan-interface101] quit
   ```

On Switch D and Switch F, enable MLD in the same way Switch A is configured. (Details not shown.)

6. Configure IPv6 admin-scoped zone boundaries:

   # On Switch B, configure VLAN-interface 102 and VLAN-interface 103 as the boundaries of IPv6 admin-scoped zone 1.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast ipv6 boundary scope 4
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] multicast ipv6 boundary scope 4
[SwitchB-Vlan-interface103] quit
```

   # On Switch C, configure VLAN-interface 104 and VLAN-interface 104 as the boundaries of IPv6 admin-scoped zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] multicast ipv6 boundary scope 4
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 105
[SwitchC-Vlan-interface105] multicast ipv6 boundary scope 4
[SwitchC-Vlan-interface105] quit
```

7. Configure C-BSRs and C-RPs:

   # On Switch B, configure the C-BSR service scope as IPv6 admin-scoped zone 1, and configure VLAN-interface 101 as a C-BSR for this zone.

```
[SwitchB] pim ipv6
[SwitchB-pim6] c-bsr scope 4
[SwitchB-pim6] c-bsr 1002::2
```

   # On Switch B, configure VLAN-interface 101 as a C-RP for IPv6 admin-scoped zone 1.

```
[SwitchB-pim6] c-rp 1002::2 scope 4
[SwitchB-pim6] quit
```

   # On Switch C, configure the C-BSR service scope as IPv6 admin-scoped zone 2, and configure VLAN-interface 104 as a C-BSR for this zone.

```
[SwitchC] pim ipv6
[SwitchC-pim6] c-bsr scope 4
[SwitchC-pim6] c-bsr 1007::1
```

   # On Switch C, configure VLAN-interface 104 as a C-RP for IPv6 admin-scoped zone 2.

```
[SwitchC-pim6] c-rp 1007::1 scope 4
[SwitchC-pim6] quit
```

   # On Switch E, configure VLAN-interface 102 as a C-BSR and a C-RP for the IPv6 global-scoped zone.

```
<SwitchE> system-view
[SwitchE] pim ipv6
[SwitchE-pim6] c-bsr scope global
[SwitchE-pim6] c-bsr 1003::2
[SwitchE-pim6] c-rp 1003::2
[SwitchE-pim6] quit
```

Verifying the configuration

1. Verify that the BSR has been elected and the local C-RP configuration in each zone has taken effect:

   # On Switch B, display information about the BSR and the locally configured C-RP.

```
[SwitchB] display pim ipv6 bsr-info
 VPN-Instance: public net
 Elected BSR Address: 1002::2
     Priority: 64
     Hash mask length: 126
     State: Elected
     Scope: 4
     Uptime: 00:03:13
     Next BSR message scheduled at: 00:00:09
 Elected BSR Address: 1003::2
     Priority: 10
     Hash mask length: 128
     State: Accept Preferred
     Scope: 14
     Uptime: 00:00:51
     Expires: 00:02:00
 Candidate BSR Address: 1002::2
     Priority: 64
     Hash mask length: 126
     State: Elected
     Scope: 4

 Candidate RP: 1002::2(Vlan-interface101)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:59
```

   # On Switch C, display information about the BSR and the locally configured C-RP.

```
[SwitchC] display pim ipv6 bsr-info
 VPN-Instance: public net
 Elected BSR Address: 1007::1
     Priority: 64
     Hash mask length: 126
     State: Elected
     Scope: 4
     Uptime: 00:03:13
     Next BSR message scheduled at: 00:00:09
 Elected BSR Address: 1003::2
     Priority: 10
     Hash mask length: 128
     State: Accept Preferred
     Scope: 14
```

```
     Uptime: 00:00:51
     Expires: 00:02:00
 Candidate BSR Address: 1007::1
     Priority: 64
     Hash mask length: 126
     State: Elected
     Scope: 4

 Candidate RP: 1007::1(Vlan-interface106)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:59
```

On Switch E, display information about the BSR and the locally configured C-RP.

```
[SwitchE] display pim ipv6 bsr-info
 VPN-Instance: public net
 Elected BSR Address: 1003::2
     Priority: 10
     Hash mask length: 128
     State: Elected
     Scope: 14
     Uptime: 00:00:51
     Next BSR message scheduled at: 00:00:42
 Candidate BSR Address: 1003::2
     Priority: 10
     Hash mask length: 128
     State: Elected
     Scope: 14

 Candidate RP: 1003::2(Vlan-interface102)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:59
```

2. Verify that the RP has been elected in each zone to provide services for different IPv6 multicast groups:

Display RP information on Switch B.

```
[SwitchB] display pim ipv6 rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 prefix/prefix length: FF04::/16
     RP: 1002::2 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:07:46
     Expires: 00:01:44

 prefix/prefix length: FF0E::/16
```

```
     RP: 1003::2
     Priority: 192
     HoldTime: 150
     Uptime: 00:03:36
     Expires: 00:02:04

 prefix/prefix length: FF14::/16
     RP: 1002::2 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:07:47
     Expires: 00:01:43

prefix/prefix length: FF1E::/16
     RP: 1003::2
     Priority: 192
     HoldTime: 150
     Uptime: 00:09:13
     Expires: 00:02:27
```

The output for **FF24::/16** to **FFF4::/16** and **FF2E::/16** to **FFFE::/16** is omitted here.

Display RP information on Switch C.

```
[SwitchC] display pim ipv6 rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 prefix/prefix length: FF04::/16
     RP: 1007::1 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:07:46
     Expires: 00:01:44

 prefix/prefix length: FF0E::/16
     RP: 1003::2
     Priority: 192
     HoldTime: 150
     Uptime: 00:03:36
     Expires: 00:02:04

 prefix/prefix length: FF14::/16
     RP: 1007::1 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:07:47
     Expires: 00:01:43

prefix/prefix length: FF1E::/16
     RP: 1003::2
     Priority: 192
```

```
     HoldTime: 150
     Uptime: 00:09:13
     Expires: 00:02:27
```

The output for **FF24::/16** to **FFF4::/16** and **FF2E::/16** to **FFFE::/16** is omitted here.

Display RP information on Switch E.

```
[SwitchE] display pim ipv6 rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 prefix/prefix length: FF0E::/16
     RP: 1003::2 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:03:36
     Expires: 00:02:04

prefix/prefix length: FF1E::/16
     RP: 1003::2 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:09:13
     Expires: 00:02:27
```

The output for **FF2E::/16** to **FFFE::/16** is omitted here.

Display RP information on Switch F.

```
[SwitchF] display pim ipv6 rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 prefix/prefix length: FF0E::/16
     RP: 1003::2
     Priority: 192
     HoldTime: 150
     Uptime: 00:03:35
     Expires: 00:02:02

prefix/prefix length: FF1E::/16
     RP: 1003::2
     Priority: 192
     HoldTime: 150
     Uptime: 00:09:13
     Expires: 00:02:22
```

The output for **FF2E::/16** to **FFFE::/16** is omitted.

The output shows the following:

- When a host in IPv6 admin-scoped zone 1 joins an IPv6 multicast group in the range of **FF04::/16** to **FFF4::/16**, the RP (Switch B) provides services for this multicast group locally.
- When a host in IPv6 admin-scoped zone 2 joins an IPv6 multicast group in the range of **FF04::/16** to **FFF4::/16**, the RP (Switch C) provides services for this multicast group locally.

- When a host in an IPv6 admin-scoped zone or the global-scoped zone joins an IPv6 multicast group in the range of **FF0E::/16** to **FFFE::/16**, the RP (Switch E) provides services for this multicast group.

Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 pim ipv6 sm
#
interface Vlan-interface101
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
pim ipv6
 c-bsr admin-scope
#
```

- Switch B:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 101 to 103
#
vlan 200
#
interface Vlan-interface101
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface102
```

```
 ipv6 address 1003::1/64
 ospfv3 1 area 0.0.0.0
 multicast ipv6 boundary scope 4
 pim ipv6 sm
#
interface Vlan-interface103
 ipv6 address 1004::1/64
 ospfv3 1 area 0.0.0.0
 multicast ipv6 boundary scope 4
 pim ipv6 sm
#
interface Vlan-interface200
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
pim ipv6
 c-bsr admin-scope
 c-bsr scope 4
 c-bsr 1002::2
 c-rp 1002::2 scope 4
#
```

- Switch C:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 104 to 106
#
vlan 300
#
interface Vlan-interface104
 ipv6 address 1005::1/64
 ospfv3 1 area 0.0.0.0
 multicast ipv6 boundary scope 4
 pim ipv6 sm
#
interface Vlan-interface105
 ipv6 address 1006::1/64
 ospfv3 1 area 0.0.0.0
 multicast ipv6 boundary scope 4
 pim ipv6 sm
#
```

```
interface Vlan-interface106
 ipv6 address 1007::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface300
 ipv6 address 3001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
pim ipv6
 c-bsr admin-scope
 c-bsr scope 4
 c-bsr 1007::1
 c-rp 1007::1 scope 4
#
```

- Switch D:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 106
#
vlan 400
#
interface Vlan-interface106
 ipv6 address 1007::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface400
 ipv6 address 4001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 pim ipv6 sm
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
#
pim ipv6
 c-bsr admin-scope
#
```

- Switch E:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 102
#
vlan 105
#
vlan 500
#
interface Vlan-interface102
 ipv6 address 1003::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface105
 ipv6 address 1006::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface500
 ipv6 address 5001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
#
pim ipv6
 c-bsr admin-scope
 c-bsr scope 14
 c-bsr hash-length 128
 c-bsr priority 10
 c-bsr 1003::2
 c-rp 1003::2
#
```

- Switch F:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 103 to 104
#
vlan 600
```

```
#
interface Vlan-interface103
 ipv6 address 1004::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface104
 ipv6 address 1005::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface600
 ipv6 address 6001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 6.6.6.6
 area 0.0.0.0
#
pim ipv6
 c-bsr admin-scope
#
```

Example: Configuring IPv6 PIM-SSM

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 93:

- All switches are Layer 3 switches, and they run OSPFv3.
- Multicast sources, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.
- The receiver hosts in the user networks support MLDv2.

Configure IPv6 PIM-SSM on each switch, so that the receiver hosts can receive VOD streams destined for an IPv6 multicast group in the IPv6 SSM group range **FF3E::/64** from a specific IPv6 multicast source.

Figure 93 Network diagram

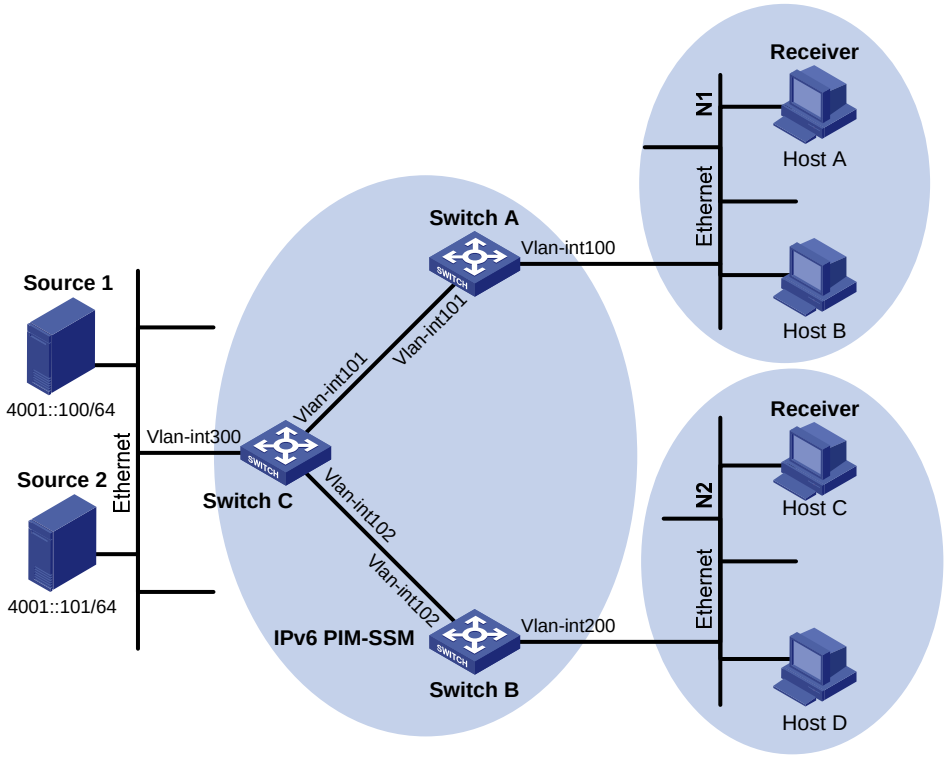


Table 6 shows the interface and IP address assignment, and network topology scheme.

Table 6 Interface and IP address assignment

Device	Interface	IPv6 address
Switch A	VLAN-interface 100	1001::1/64
Switch A	VLAN-interface 101	1002::1/64
Switch B	VLAN-interface 200	2001::1/64
Switch B	VLAN-interface 102	2002::1/64
Switch C	VLAN-interface 300	4001::1/64
Switch C	VLAN-interface 101	1002::2/64
Switch C	VLAN-interface 102	2002::2/64

Requirements analysis

For IPv6 PIM-SSM to provide services for IPv6 multicast groups in the range specified in the network requirements, you must specify this range on each Layer 3 switch.

In IPv6 SSM, the edge Layer 3 switch must obtain information about the specified multicast source when a host joins an IPv6 multicast group. To meet the requirement, you must enable MLDv2 on the edge switches that connect to the user networks.

Configuration restrictions and guidelines

When a member of an IPv6 multicast group in the IPv6 SSM group range sends an MLDv1 report message, the device does not trigger a (*, G) join. In this case, you can configure MLD SSM mappings, so that IPv6 PIM-SSM can provide services for hosts that support only MLDv1.

Configuration procedures

1. Enable IPv6 forwarding on the switches.
2. Assign an IPv6 address and prefix length to each interface according to Table 6. (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)
4. Enable IPv6 multicast routing globally and configure IPv6 PIM-SSM:

   # On Switch A, enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast ipv6 routing-enable
   ```

   # On Switch A, enable IPv6 PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] pim ipv6 sm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim ipv6 sm
   [SwitchA-Vlan-interface101] quit
   ```

   # Enable IPv6 multicast routing, and IPv6 PIM-SM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)
5. Configure the IPv6 SSM group range:

   # On Switch A, configure the IPv6 SSM group range to **FF3E::/64**.

   ```
   [SwitchA] acl ipv6 number 2000
   [SwitchA-acl6-basic-2000] rule permit source ff3e:: 64
   [SwitchA-acl6-basic-2000] quit
   [SwitchA] pim ipv6
   [SwitchA-pim6] ssm-policy 2000
   [SwitchA-pim6] quit
   ```

   # On Switch B and Switch C, configure the IPv6 SSM group ranges in the same way Switch A is configured. (Details not shown.)
6. Enable MLDv2 on the interfaces connected to the stub networks **N1** and **N2**:

   # On Switch A, enable MLDv2 on VLAN-interface 100.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] mld enable
   [SwitchA-Vlan-interface100] mld version 2
   [SwitchA-Vlan-interface100] quit
   ```

   # On Switch B, enable MLDv2 on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

To verify that correct (S, G) entries are created on switches:

1. Send MLDv2 report from Host A to join the IPv6 multicast group **FF3E::101** and specify the IPv6 multicast source as **4001::100/64**.
2. Use the **display pim ipv6 routing-table** command to display IPv6 PIM routing tables on Switch A and Switch C:

   # Display the PIM routing table on Switch A.

```
[SwitchA] display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (4001::100, FF3E::101)
     Protocol: pim-ssm, Flag:
     UpTime: 00:00:11
     Upstream interface: Vlan-interface101
         Upstream neighbor: FE80::223:89FF:FE5F:958C
         RPF prime neighbor: FE80::223:89FF:FE5F:958C
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface100
             Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

   # Display the PIM routing table on Switch C.

```
[SwitchC] display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (4001::100, FF3E::101)
     Protocol: pim-ssm, Flag: LOC
     UpTime: 00:08:02
     Upstream interface: Vlan-interface300
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface101
             Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25
```

   The output shows that Switch A builds an SPT toward the IPv6 multicast source. Switches on the SPT path (Switch A and Switch D) generate (S, G) entries.

Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
```

```
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 mld version 2
 pim ipv6 sm
#
interface Vlan-interface101
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
pim ipv6
 ssm-policy 2000
#
```

- Switch B:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface200
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 mld version 2
```

```
 pim ipv6 sm
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
pim ipv6
 ssm-policy 2000
#
```

- Switch C:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface102
 ipv6 address 2002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface300
 ipv6 address 4001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
pim ipv6
 ssm-policy 2000
#
```

IRF configuration examples

This chapter provides examples for deploying LACP MAD-enabled four-chassis IRF fabrics and BFD MAD-enabled four-chassis IRF fabrics.

IRF technology creates a large switching system called an "IRF fabric" from multiple devices to provide data center class availability and scalability. IRF virtualization technology offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

An IRF fabric appears as one node and is accessible at a single IP address.

General configuration restrictions and guidelines

When you configure IRF, follow the restrictions and guidelines in this section.

This section provides only the basic restrictions and guidelines that ensure a successful IRF deployment. For complete information, see *HP 7500 Switch Series IRF Configuration Guide*.

IRF fabric size

A 7510 IRF fabric can have only up to two chassis. Other models can form four-member IRF fabrics.

Hardware requirements

- The member chassis must be the same model.
- Only 10-GE and 40-GE ports can be used for IRF connection. You must purchase 10-GE or 40-GE LPUs, as well as compatible transceiver modules and cables. For more information, see *HP 7500 Switch Series Installation Guide*.
- Every IRF member chassis must have at least one MPU. Do not remove all MPUs of a member chassis while the IRF fabric is operating.

Software requirements

All IRF member devices must run the same system software image version.

IRF physical ports and connection requirements

IMPORTANT:

When you connect two neighboring IRF members, you must connect the physical ports of IRF-port 1 on one member to the physical ports of IRF-port 2 on the other. No intermediate devices are allowed between neighboring members.

If you are using a 40-GE port for IRF connection, HP recommends completing the port split or combination operation before adding the switch to an IRF fabric. As of Release 6703, you can use the **using tengige** command or the **using fortygige** command to split 40-GE QSFP+ ports on SF cards into

10-GE ports or recombine 10-GE ports into 40-GE ports. These operations require a card reboot. To perform these operations in an IRF fabric, make sure you understand the impact on the IRF fabric topology. For more information about 40-GE port split and combination operations, see *HP 7500 Switch Series Layer 2—LAN Switching Configuration Guide*.

Topologies

The IRF fabric can use a daisy chain topology or ring topology. To use the ring topology, you must have three or four chassis.

MAD requirements

You must configure LACP MAD, BFD MAD, or both on an IRF fabric. To choose a suitable MAD mechanism for your network, use Table 7.

Table 7 A comparison of the MAD mechanisms

MAD mechanism	Advantages	Disadvantages	Application scenario
LACP MAD	• Detection speed is fast. • Requires no MAD-dedicated physical ports or interfaces.	Requires an intermediate HP device that supports LACP MAD packets.	Link aggregation is used between the IRF fabric and its upstream or downstream device.
BFD MAD	• Detection speed is fast. • No intermediate device is required. • Intermediate device, if used, can come from any vendor.	• Requires MAD dedicated physical ports and Layer 3 interfaces, which cannot be used for transmitting user traffic. • If no intermediate device is used, the IRF members must be fully meshed. • If an intermediate device is used, every IRF member must connect to the intermediate device.	• Suitable for various network scenarios. • If no intermediate device is used, this mechanism is only suitable for IRF fabrics that have a small number of members that are geographically close to one another.

Example: Setting up a four-chassis LACP MAD-enabled IRF fabric

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

To improve network performance and decrease topology complexity without decreasing availability, use a four-chassis 7500 IRF fabric (see Figure 95) to replace the switches (see Figure 94) at the distribution layer of the data center.

Use LACP MAD to detect IRF split.

The IRF fabric provides Layer 2 forwarding services, and the core routers provide gateway services for servers.

Figure 94 Network diagram before IRF deployment

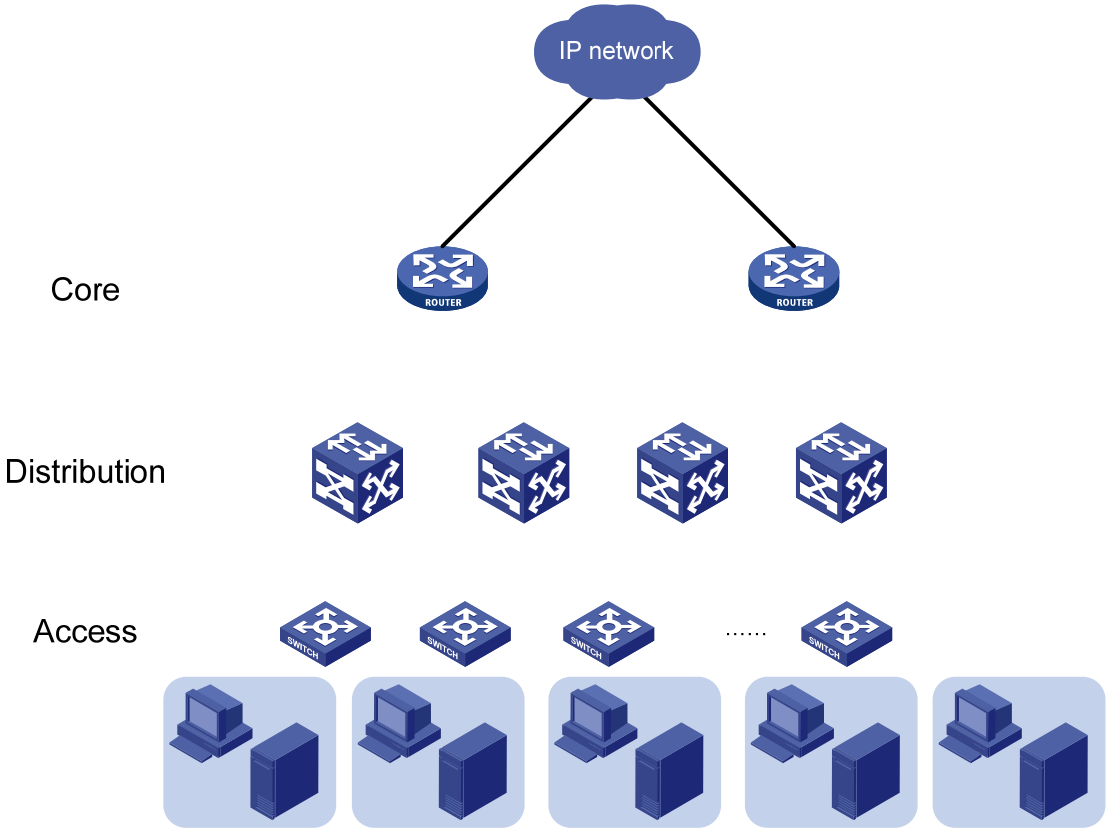
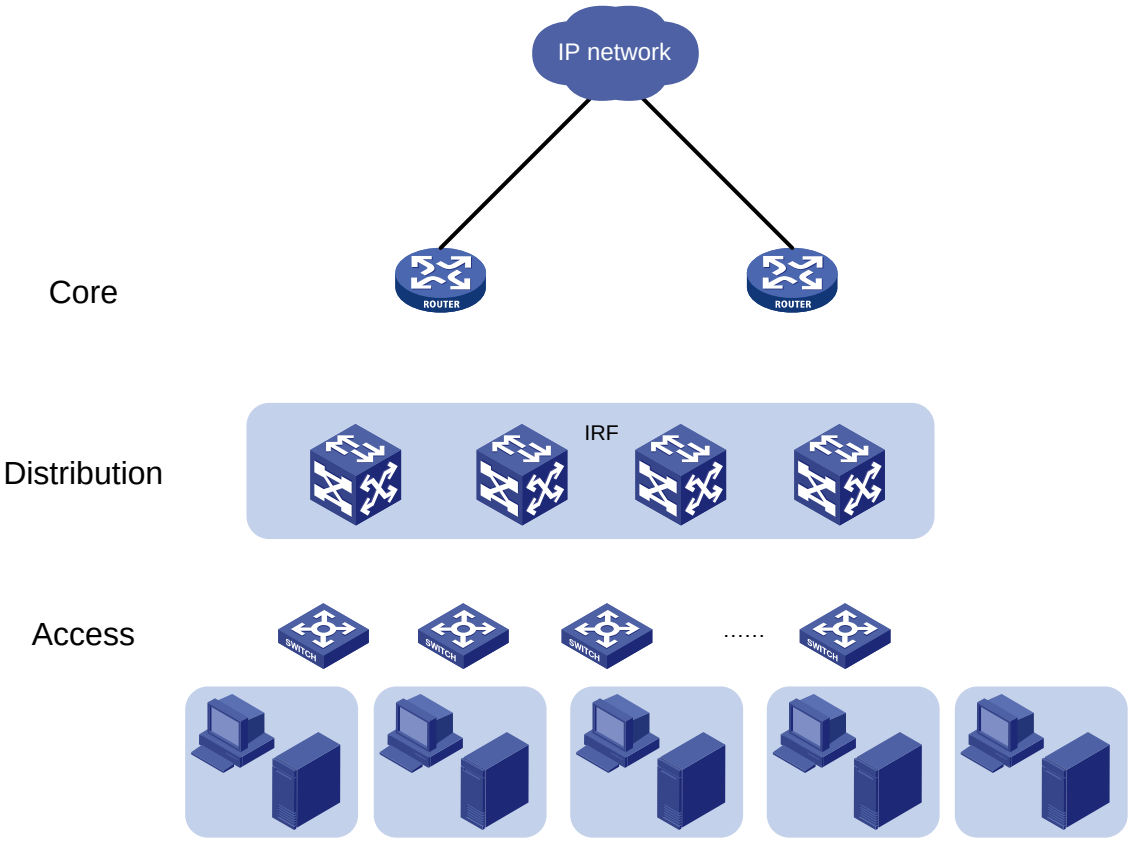


Figure 95 Network diagram after IRF deployment



Requirements analysis

The requirements in this example include the following categories:

- IRF setup
- LACP MAD configuration
- Software feature configuration

IRF setup

To set up an IRF fabric, refer to the items in Table 8.

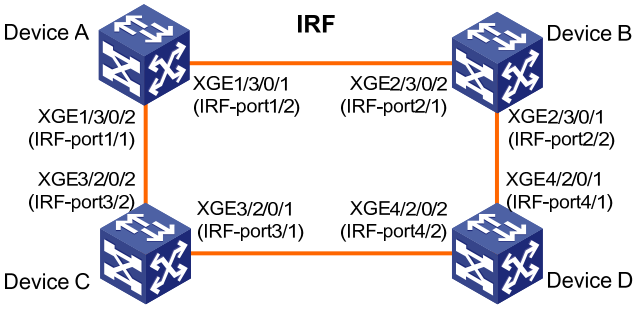
Table 8 Basic IRF setup

Item	Analysis	Choice in this example
Topology	You can use a ring or daisy chain topology for a three- or four-chassis IRF fabric. For reliability, use the ring topology as long as possible.	Ring topology (see Table 8Figure 96).
Member ID assignment	IRF member IDs must be unique.	• **Device A**—1. • **Device B**—2. • **Device C**—3. • **Device D**—4.

Item	Analysis	Choice in this example
Master device	IRF members elect a master automatically. To affect the election result, you could assign the desired master chassis higher member priority.	Device A.
IRF port bindings	For two neighboring IRF members, you must connect the physical ports of IRF-port 1 on one member to the physical ports of IRF-port 2 on the other. When you bind physical ports to IRF ports, you must make sure the bindings are consistent with the physical connections. For reliability, bind multiple physical ports to an IRF port. These ports will automatically aggregate for load balancing and redundancy.	See Table 8Figure 96.

To reduce the number of reboots during IRF setup, configure IRF port bindings, member ID, and member priority on each chassis before changing their operating mode to IRF.

Figure 96 IRF fabric topology



NOTE:

This figure shows the port numbers in IRF mode. In IRF mode, a physical port number has four segments, with the IRF member ID as the first segment. In standalone mode, a physical port number does not include the IRF member ID.

LACP MAD configuration

IMPORTANT:

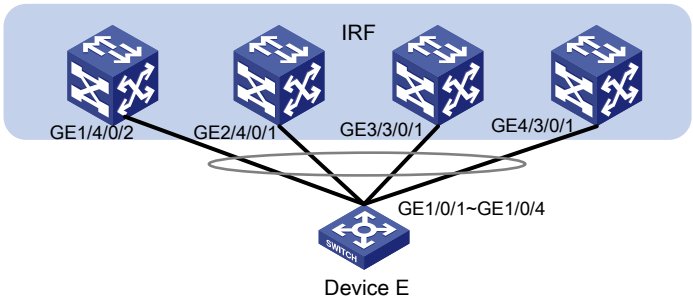
For LACP MAD to run correctly, you must make sure the intermediate device supports extended LACPDUs for LACP MAD.

You can use LACP MAD if the IRF fabric has a dynamic Ethernet link aggregation with a device that can recognize LACP MAD packets, as shown in Figure 97. LACP MAD cannot run on a static (or manual) link aggregation.

You do not need to run LACP MAD on all link aggregations. You can detect IRF split effectively by running LACP MAD on one dynamic link aggregation. This example uses the link aggregation to Device E for LACP MAD.

On the intermediate devices, you only need to configure a dynamic link aggregation for connecting to the IRF fabric.

Figure 97 LACP MAD



Software feature configuration

On the IRF fabric, you configure software features in the same way as you do with a standalone switch.

To connect to the downstream switches and the upstream egress routers, set up multichassis link aggregations for link backup, as shown in Figure 98. A link aggregation could span one member chassis, some of the member chassis, or all member chassis, depending on the link redundancy requirements and number of available links.

NOTE:

The link aggregation used for LACP MAD must span all member chassis.

On the core routers, use VRRP to improve gateway availability. If the routers are IRF-capable HP Layer 3 switches, you could combine them into an IRF fabric to simplify the network topology.

Figure 98 Connection diagram for the IRF fabric in a Layer 2 network

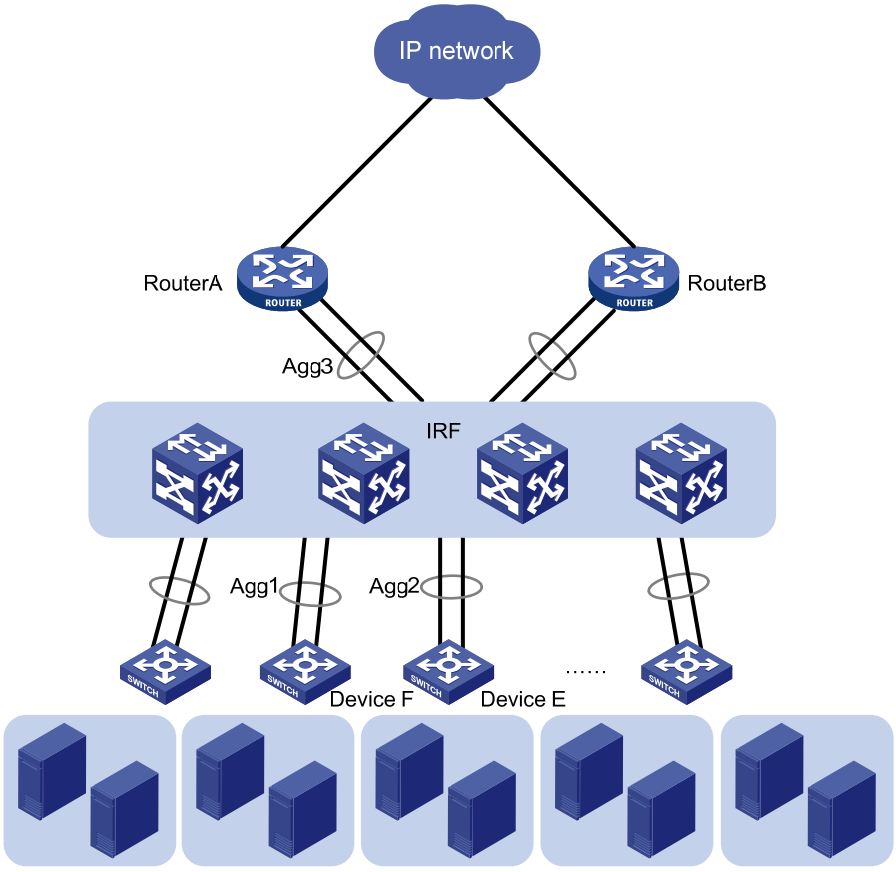


Table 9 Link aggregations and VLAN assignment scheme

Aggregate interface	VLANs	Member ports
Router A:		
Bridge-Aggregation 3	VLAN 100 VLAN 101 VLAN 200 VLAN 201	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4
IRF fabric:		
Bridge-Aggregation 1	VLAN 200 VLAN 201	GigabitEthernet1/4/0/10 GigabitEthernet2/4/0/10 GigabitEthernet3/3/0/3 GigabitEthernet4/3/0/4
Bridge-Aggregation 2	VLAN 100 VLAN 101	GigabitEthernet1/4/0/2 GigabitEthernet2/4/0/1 GigabitEthernet3/3/0/1 GigabitEthernet4/3/0/1
Bridge-Aggregation 3	VLAN 100 VLAN 101 VLAN 200 VLAN201	GigabitEthernet1/4/0/11 GigabitEthernet2/4/0/11 GigabitEthernet3/3/0/11 GigabitEthernet4/3/0/11
Device E:		
Bridge-Aggregation 2	VLAN 100 VLAN 101	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4
Device F:		
Bridge-Aggregation 1	VLAN 200 VLAN 201	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4

Configuration restrictions and guidelines

When you configure LACP MAD and IRF port bindings, follow the restrictions and guidelines in this section.

LACP MAD

When you configure LACP MAD on a link aggregation, follow these restrictions and guidelines:

- The link aggregation must use dynamic aggregation mode.
- The link aggregation must have at least one member link from each member chassis.
- If the intermediate device is also an IRF fabric, you must assign the two IRF fabrics different domain IDs to ensure correct split detection.

IRF port binding

When you bind physical ports to an IRF ports, follow these restrictions and guidelines:

- IRF physical ports must be set to bridge mode (the default).

- When you bind physical ports to an IRF port, you must set all the physical ports to operate in the same mode: normal or enhanced. If you do not specify a mode, the normal mode applies.
- The physical ports of two connected IRF ports must operate in the same mode: normal or enhanced.
- To use the MPLS L2VPN or VPLS function in an IRF fabric, you must specify the **mode enhanced** option when binding IRF ports.

Configuration procedures

Setting up the IRF fabric

1. Configure Device A:

   # Assign member ID 1 to Device A.

```
<Sysname> system-view
[Sysname] irf member 1
 Info: Member ID change will take effect after the member reboots and operates in IRF mode.
```

   # Bind Ten-GigabitEthernet 3/0/2 to IRF-port 1, and bind Ten-GigabitEthernet 3/0/1 to IRF-port 2.

> IMPORTANT:
>
> To avoid traffic forwarding problems, shut down physical ports before binding them to an IRF port.

```
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 3/0/2
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 3/0/1
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
```

   # Assign an IRF member priority of 31 to Device A. This high priority makes sure Device A can be elected as the master.

```
[Sysname] irf priority 31
```

   # Save the running configuration before changing the operating mode to IRF. The mode change requires a system reboot, which can cause all unsaved settings to be lost.

```
[Sysname] quit
<Sysname> save
```

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device A reboots to form a one-chassis IRF fabric.

2. Configure Device B:

Assign member ID 2 to Device B.

```
<Sysname> system-view
[Sysname] irf member 2
 Info: Member ID change will take effect after the member reboots and operates in IRF
mode.
```

Bind Ten-GigabitEthernet 3/0/2 to IRF-port 1, and bind Ten-GigabitEthernet 3/0/1 to IRF-port 2.

```
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 3/0/2
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 3/0/1
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device B to Device A, as shown in Figure 96.

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
```

```
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device B reboots to join the IRF fabric. A two-chassis IRF fabric is formed.

3. Configure Device C:

Assign member ID 3 to Device C.

```
<Sysname> system-view
[Sysname] irf member 3
 Info: Member ID change will take effect after the member reboots and operates in IRF
mode.
```

Bind Ten-GigabitEthernet 2/0/1 to IRF-port 1, and bind Ten-GigabitEthernet 2/0/2 to IRF-port 2.

```
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 2/0/1
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 2/0/2
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device C to Device A and Device D, as shown in Figure 96.

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
```

```
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device C reboots to join the IRF fabric.

4. Configure Device D:

Assign member ID 4 to Device D.

```
<Sysname> system-view
[Sysname] irf member 4
 Info: Member ID change will take effect after the member reboots and operates in IRF
mode.
```

Bind Ten-GigabitEthernet 2/0/1 to IRF-port 1, and bind Ten-GigabitEthernet 2/0/2 to IRF-port 2.

```
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 2/0/1
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 2/0/2
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device D to Device B and Device C, as shown in Figure 96.

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
```

```
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

Configuring LACP MAD

1. Configure the IRF fabric:

   # Assign domain ID 1 to the IRF fabric.

```
<Sysname> system-view
[Sysname] irf domain 1
```

   # Create Bridge-Aggregation 2, set its aggregation mode to dynamic, and enable LACP MAD.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 2
[Sysname-Bridge-Aggregation2] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation2] mad enable
You need to assign a domain ID (range: 0-4294967295)
 [Current domain is: 1]:
 The assigned  domain ID is: 1
 Info: MAD LACP only enable on dynamic aggregation interface.
[Sysname-Bridge-Aggregation2] quit
```

   # Assign GigabitEthernet 1/4/0/2, GigabitEthernet 2/4/0/1, GigabitEthernet 3/3/0/1, and GigabitEthernet 4/3/0/1 to the aggregate interface.

```
[Sysname] interface gigabitethernet 1/4/0/2
[Sysname-GigabitEthernet1/4/0/2] port link-aggregation group 2
[Sysname-GigabitEthernet1/4/0/2] quit
[Sysname] interface gigabitethernet 2/4/0/1
[Sysname-GigabitEthernet2/4/0/1] port link-aggregation group 2
[Sysname-GigabitEthernet2/4/0/1] quit
[Sysname] interface gigabitethernet 3/3/0/1
[Sysname-GigabitEthernet3/3/0/1] port link-aggregation group 2
[Sysname-GigabitEthernet3/3/0/1] quit
[Sysname] interface gigabitethernet 4/3/0/1
[Sysname-GigabitEthernet4/3/0/1] port link-aggregation group 2
[Sysname-GigabitEthernet4/3/0/1] quit
```

2. Configure Device E (the intermediate device):

   CAUTION:

   If Device E is also an IRF fabric, you must assign the two IRF fabrics different domain IDs to ensure correct split detection. False detection of IRF split can interrupt forwarding service.

   # Create a dynamic aggregate interface.

```
<DeviceE> system-view
[DeviceE] interface bridge-aggregation 2
[DeviceE-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceE-Bridge-Aggregation2] quit
```

   # Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the aggregate interface.

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

Configuring software features

1. Configure Router A:

   # Create VLANs 100, 101, 200, and 201.

   ```
   <RouterA> system-view
   [RouterA] vlan 100 to 101
   [RouterA] vlan 200 to 201
   ```

   # Create Bridge-Aggregation 3 and set its aggregation mode to dynamic.

   ```
   [RouterA] interface bridge-aggregation 3
   [RouterA-Bridge-Aggregation3] link-aggregation mode dynamic
   [RouterA-Bridge-Aggregation3] quit
   ```

   # Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the aggregation group for Bridge-Aggregation 3.

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

   # Configure Bridge-Aggregation 3 as a trunk port, remove it from VLAN 1, and assign it to VLANs 100, 101, 200, and 201.

   ```
   [RouterA] interface bridge-aggregation 3
   [RouterA-Bridge-Aggregation3] port link-type trunk
   [RouterA-Bridge-Aggregation3] port trunk permit vlan 100 101 200 201
   Please wait... Done.
   [RouterA-Bridge-Aggregation3] undo port trunk permit vlan 1
   Please wait... Done.
   Configuring GigabitEthernet1/0/1... Done.
   Configuring GigabitEthernet1/0/2... Done.
   Configuring GigabitEthernet1/0/3... Done.
   ```

```
Configuring GigabitEthernet1/0/4... Done.
[RouterA-Bridge-Aggregation3] quit
```

NOTE:

By default, all ports are in VLAN 1. To prevent VLAN 1 traffic from passing through a trunk or hybrid port, you must remove the port from the VLAN.

Create VLAN-interfaces 100, 101, 200, and 201, and assign the interfaces IP addresses for providing gateway service. (Details not shown.)

2. Configure the IRF fabric:

Create Bridge-Aggregation 1 and set its link aggregation mode to dynamic.

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

Assign GigabitEthernet 1/4/0/10, GigabitEthernet 2/4/0/10, GigabitEthernet 3/3/0/3, and GigabitEthernet 4/3/0/4 to the aggregation group for Bridge-Aggregation 1.

```
[Sysname] interface gigabitethernet 1/4/0/10
[Sysname-GigabitEthernet1/4/0/10] port link-aggregation group 1
[Sysname-GigabitEthernet1/4/0/10] quit
[Sysname] interface gigabitethernet 2/4/0/10
[Sysname-GigabitEthernet2/4/0/10] port link-aggregation group 1
[Sysname-GigabitEthernet2/4/0/10] quit
[Sysname] interface gigabitethernet 3/3/0/3
[Sysname-GigabitEthernet3/3/0/3] port link-aggregation group 1
[Sysname-GigabitEthernet3/3/0/3] quit
[Sysname] interface gigabitethernet 4/3/0/4
[Sysname-GigabitEthernet4/3/0/4] port link-aggregation group 1
[Sysname-GigabitEthernet4/3/0/4] quit
```

Configure Bridge-Aggregation 1 as a trunk port, remove it from VLAN 1, and assign it to VLANs 200 and 201.

```
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type trunk
[Sysname-Bridge-Aggregation1] port trunk permit vlan 200 201
Please wait... Done.
[Sysname-Bridge-Aggregation1] undo port trunk permit vlan 1
Please wait... Done.
Configuring GigabitEthernet1/4/0/10... Done.
Configuring GigabitEthernet2/4/0/10... Done.
Configuring GigabitEthernet3/3/0/3... Done.
Configuring GigabitEthernet4/3/0/4... Done.
[Sysname-Bridge-Aggregation1] quit
```

Configure Bridge-Aggregation 2 as a trunk port, remove it from VLAN 1, and assign it to VLANs 100 and 101. (Bridge-Aggregation 2 is the interface used for LACP MAD.)

```
[Sysname] interface bridge-aggregation 3
[Sysname-Bridge-Aggregation3] port link-type trunk
[Sysname-Bridge-Aggregation3] port trunk permit vlan 100 101
Please wait... Done.
```

```
[Sysname-Bridge-Aggregation3] undo port trunk permit vlan 1
Please wait... Done.
Configuring GigabitEthernet1/4/0/2... Done.
Configuring GigabitEthernet2/4/0/1... Done.
Configuring GigabitEthernet3/3/0/1... Done.
Configuring GigabitEthernet4/3/0/1... Done.
[Sysname-Bridge-Aggregation3] quit
```

Create Bridge-Aggregation 3 and set its link aggregation mode to dynamic.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 3
[Sysname-Bridge-Aggregation3] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/4/0/11, GigabitEthernet 2/4/0/11, GigabitEthernet 3/3/0/11, and GigabitEthernet 4/3/0/11 to the aggregation group for Bridge-Aggregation 3.

```
[Sysname] interface gigabitethernet 1/4/0/11
[Sysname-GigabitEthernet1/4/0/11] port link-aggregation group 3
[Sysname-GigabitEthernet1/4/0/11] quit
[Sysname] interface gigabitethernet 2/4/0/11
[Sysname-GigabitEthernet2/4/0/11] port link-aggregation group 3
[Sysname-GigabitEthernet2/4/0/11] quit
[Sysname] interface gigabitethernet 3/3/0/11
[Sysname-GigabitEthernet3/3/0/11] port link-aggregation group 3
[Sysname-GigabitEthernet3/3/0/11] quit
[Sysname] interface gigabitethernet 4/3/0/11
[Sysname-GigabitEthernet4/3/0/11] port link-aggregation group 3
[Sysname-GigabitEthernet4/3/0/11] quit
```

Configure Bridge-Aggregation 3 as a trunk port, remove it from VLAN 1, and assign it to VLANs 100, 101, 200, and 201.

```
[Sysname] interface bridge-aggregation 3
[Sysname-Bridge-Aggregation3] port link-type trunk
[Sysname-Bridge-Aggregation3] port trunk permit vlan 100 101 200 201
Please wait... Done.
[Sysname-Bridge-Aggregation3] undo port trunk permit vlan 1
Please wait... Done.
Configuring GigabitEthernet1/4/0/11... Done.
Configuring GigabitEthernet2/4/0/11... Done.
Configuring GigabitEthernet3/3/0/11... Done.
Configuring GigabitEthernet4/3/0/11... Done.
[Sysname-Bridge-Aggregation3] quit
```

3. Configure Device E:

Configure Bridge-Aggregation 2 as a trunk port, remove it from VLAN 1, and assign it to VLANs 100 and 101. (Bridge-Aggregation 2 is the interface used for LACP MAD.)

```
[DeviceE] interface bridge-aggregation 3
[DeviceE-Bridge-Aggregation3] port link-type trunk
[DeviceE-Bridge-Aggregation3] port trunk permit vlan 100 101
Please wait... Done.
[DeviceE-Bridge-Aggregation3] undo port trunk permit vlan 1
```

```
Please wait... Done.
Configuring GigabitEthernet1/4/0/2... Done.
Configuring GigabitEthernet2/4/0/1... Done.
Configuring GigabitEthernet3/3/0/1... Done.
Configuring GigabitEthernet4/3/0/1... Done.
[Sysname-Bridge-Aggregation3] quit
```

4. Configure Device F:

   # Create Bridge-Aggregation 1 and set its link aggregation mode to dynamic.

```
<DeviceF> system-view
[DeviceF] interface bridge-aggregation 1
[DeviceF-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceF-Bridge-Aggregation2] quit
```

   # Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the aggregation group for Bridge-Aggregation 1.

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

   # Configure Bridge-Aggregation 1 as a trunk port, remove it from VLAN 1, and assign it to VLANs 200 and 201.

```
[DeviceF] interface bridge-aggregation 1
[DeviceF-Bridge-Aggregation1] port link-type trunk
[DeviceF-Bridge-Aggregation1] port trunk permit vlan 200 201
Please wait... Done.
[DeviceF-Bridge-Aggregation1] undo port trunk permit vlan 1
Please wait... Done.
Configuring GigabitEthernet1/4/0/10... Done.
Configuring GigabitEthernet2/4/0/10... Done.
Configuring GigabitEthernet3/3/0/3... Done.
Configuring GigabitEthernet4/3/0/4... Done.
[DeviceF-Bridge-Aggregation1] quit
```

Verifying the configuration

Verify the IRF setup, multichassis link aggregations, ring topology, and LACP MAD.

Verifying the IRF setup

Execute the **display irf** command to verify that the IRF fabric has been formed.

```
[Sysname] display irf
```

```
MemberID  Slot  Role    Priority  CPU-Mac         Description
 *+1      1     Master  31        00e0-fc0f-8c02  ---
   2      4     Standby 1         00e0-fc0f-8c17  ---
   3      7     Standby 1         00e0-fc0f-8c2c  ---
   4      1     Standby 1         00e0-fc0f-8c38  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-89bb-3034
 Auto upgrade                : yes
 Mac persistent              : always
 Domain ID                   : 0
 Auto merge                  : no
```

The output shows that the IRF fabric has four member chassis.

Execute the **display irf topology** command to verify IRF fabric connectivity.

```
[Sysname] display irf topology
                            Topology Info
 ------------------------------------------------------------------------
              IRF-Port1                IRF-Port2
 MemberID    Link       neighbor      Link       neighbor    Belong To
 1           UP         3             UP         2           00e0-fc0f-8c02
 3           UP         4             UP         1           00e0-fc0f-8c02
 4           UP         2             UP         3           00e0-fc0f-8c02
 2           UP         1             UP         4           00e0-fc0f-8c02
```

The output shows that all the IRF links are in UP state. The four-chassis IRF fabric is established.

Verifying the link backup function of multichassis aggregations

Ping the gateway address on Router A from a server.

```
C:\Users>ping 10.153.116.111 –t
```

On the IRF fabric, shut down GigabitEthernet 1/4/0/11, a member port of Bridge-Aggregation 3.

```
[Sysname] interface gigabitethernet 1/4/0/11
[Sysname-GigabitEthernet1/4/0/11] shutdown
[Sysname-GigabitEthernet1/4/0/11] quit
```

Observe the output on the configuration terminal for the server.

```
Pinging 10.153.116.111 with 32 bytes of data:

Reply from 10.153.116.111: bytes=32 time<1ms TTL=128
Reply from 10.153.116.111: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Reply from 10.153.116.111: bytes=32 time<1ms TTL=128
Reply from 10.153.116.111: bytes=32 time<1ms TTL=128
```

The output shows that the gateway address can be pinged after transient traffic disruption.

Verifying link failure protection of the ring topology

Disconnect all IRF links between two IRF member devices to verify that the IRF fabric can operate correctly as a daisy chained fabric.

Verifying the LACP MAD configuration

Disconnect two IRF connections: one between Device A and Device B, and the other between Device C and Device D. The system displays the following IRF link state and card failure error messages:

```
#May  7 09:13:42:388 2010 HP STM/4/LINK STATUS CHANGE:
#May  7 09:13:42:720 2010 HP DEVM/1/BOARD STATE CHANGES TO FAILURE:
```

The disconnect actions cause the IRF fabric to break down into two parts: IRF 1 (Device A and Device C) and IRF 2 (Device B and Device D). Because the master chassis in IRF 1 has a lower member ID than the master chassis in IRF 2, LACP MAD should set IRF 2 (Device B and Device D) in Recovery state.

Verify that LACP MAD shuts down physical network ports on Device B and Device D. The ports shut down by MAD do not include IRF physical ports and ports configured to be excluded from the shutdown action.

Verify that IRF 1 (Device A and Device C) can continue to forward traffic.

If IRF 1 fails, log in to IRF 2, and use the **mad restore** command to recover the member chassis and bring up all ports that have been shut down by LACP MAD. (You can log in from the console port on Device B or Device D. Alternatively, you can log in from a network port that is excluded from the shutdown action by using the **mad exclude interface** command.)

```
<Sysname> system-view
[Sysname] mad restore
This command will restore the device from multi-active conflict state. Continue? [Y/N]:y
Restoring from multi-active conflict state, please wait...
[Sysname]
#May  7 09:23:16:050 2010 HP IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 277872640 is Up, ifAdminStatus is 1,
ifOperStatus is 1
%May  7 09:23:16:069 2010 HP IFNET/3/LINK_UPDOWN: GigabitEthernet2/3/0/2 link status is
UP.
#May  7 09:23:16:302 2010 HP LAGG/1/AggPortRecoverActive:
 Trap 1.3.6.1.4.1.2011.5.25.25.2.4<hwAggPortActiveNotification>: Aggregation Group 2:
port member 277872640 becomes ACTIVE!
%May  7 09:23:16:322 2010 HP LAGG/5/LAGG_ACTIVE: Member port GigabitEthernet2/4/0/1 of
aggregation group BAGG2 becomes ACTIVE.
%May  7 09:23:16:370 2010 HP IFNET/3/LINK_UPDOWN: Bridge-Aggregation2 link status is UP.
%May  7 09:23:16:381 2010 HP IFNET/3/LINK_UPDOWN: Vlan-interface1 link status is UP.
%May  7 09:23:16:391 2010 HP IFNET/5/LINEPROTO_UPDOWN: Line protocol on the interface
Vlan-interface1 is UP.
```

The output shows that network connectivity of IRF 2 has been restored.

Remove all IRF 1 and IRF link failures.

Reboot IRF 1 to merge with IRF 2. When the merge completes, IRF 2 displays the following messages to show that IRF links are recovered and new members are added:

```
%May  7 09:30:12:122 2010 HP STM/6/STM_LINK_STATUS_UP:
#May  7 09:30:36:566 2010 HP DEVM/1/BOARD INSERTED:
```

Execute the **display irf** command to verify that the IRF fabric is recovered and Device B is the master.

```
<Sysname> display irf
MemberID  Slot  Role   Priority  CPU-Mac         Description
   1      1    Slave   1         00e0-fc0f-8c02  -----
 *+2      1    Master  1         00e0-fc0f-8c20  -----
   3      1    Slave   1         00e0-fc00-5801  -----
   4      1    Slave   1         00e0-fc00-3583  -----
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.
 The Bridge MAC of the IRF is: 0023-895f-954f
 Auto upgrade                : yes
 Mac persistent              : always
 Domain ID                   : 0
 Auto merge                  : no
```

Configuration files

- IRF fabric:

```
#
vlan 100 to 101
#
vlan 200 to 201
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 link-aggregation mode dynamic
#
interface Bridge-Aggregation2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 link-aggregation mode dynamic
 mad enable
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 link-aggregation mode dynamic
#
interface gigabitethernet 1/4/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-aggregation group 2
```

```
#
interface gigabitethernet 1/4/0/10
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
#
interface gigabitethernet 1/4/0/11
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
#
interface gigabitethernet 2/4/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-aggregation group 2
#
interface gigabitethernet 2/4/0/10
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
#
interface gigabitethernet 2/4/0/11
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
#
interface gigabitethernet 3/3/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-aggregation group 2
#
interface gigabitethernet 3/3/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
```

```
 port link-aggregation group 1
#
interface gigabitethernet 3/3/0/11
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
#
interface gigabitethernet 4/3/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-aggregation group 2
#
interface gigabitethernet 4/3/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
#
interface gigabitethernet 4/3/0/11
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/3/0/2 mode enhanced
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/3/0/1 mode enhanced
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/3/0/2 mode enhanced
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/3/0/1 mode enhanced
#
irf-port 3/1
 port group interface Ten-GigabitEthernet3/2/0/1 mode enhanced
#
irf-port 3/2
 port group interface Ten-GigabitEthernet3/2/0/2 mode enhanced
#
```

```
irf-port 4/1
 port group interface Ten-GigabitEthernet4/2/0/1 mode enhanced
#
irf-port 4/2
 port group interface Ten-GigabitEthernet4/2/0/2 mode enhanced
```

- Device E:

```
#
interface Bridge-Aggregation2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 link-aggregation mode dynamic
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-aggregation group 2
#
interface gigabitethernet 1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-mode bridge
 port link-aggregation group 2
#
interface gigabitethernet 1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-mode bridge
 port link-aggregation group 2
#
interface gigabitethernet 1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101
 port link-mode bridge
 port link-aggregation group 2
```

- Device F:

```
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 link-aggregation mode dynamic
#
```

```
interface gigabitethernet 1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 to 201
 port link-aggregation group 1
```

- Router A:

```
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 link-aggregation mode dynamic
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
```

```
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 101 200 to 201
 port link-aggregation group 3
```

Example: Setting up a four-chassis BFD MAD-enabled IRF fabric

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

To improve network performance and decrease topology complexity without decreasing availability, set up a four-chassis 7500 IRF fabric (Figure 100) to replace the switches (Figure 99) at the distribution layer of the data center.

Use BFD MAD to detect IRF split.

The IRF fabric provides gateway services for servers and runs OSPF.

Figure 99 Network diagram before IRF deployment

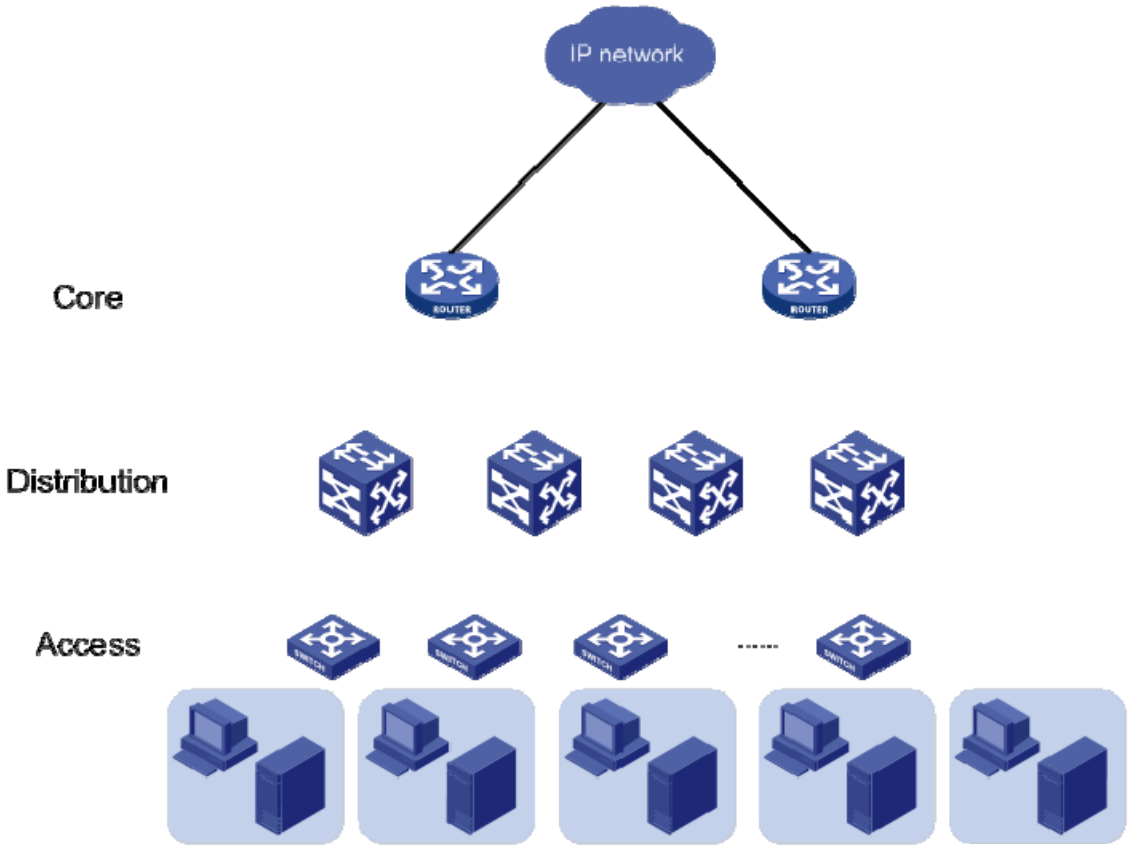
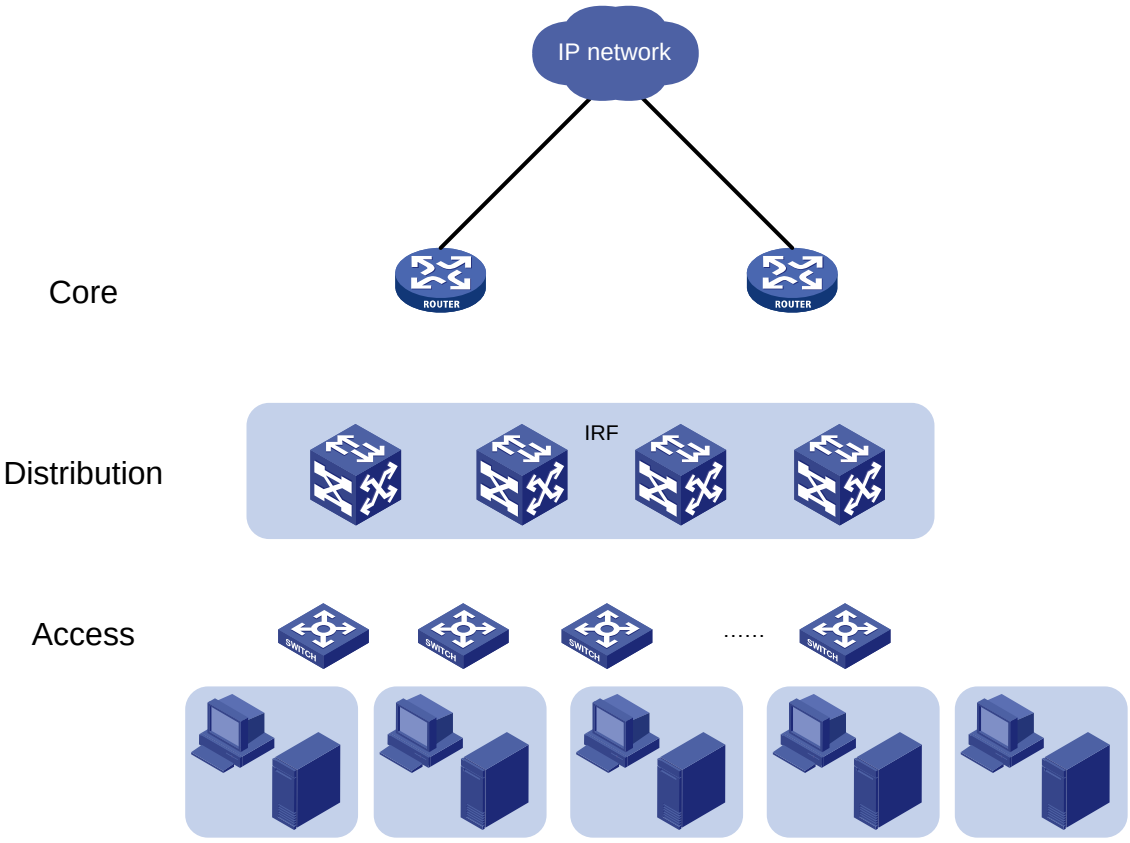


Figure 100 Network diagram after IRF deployment



Requirements analysis

The requirements in this example include the following categories:

- IRF setup
- BFD MAD configuration
- Software feature configuration

IRF setup

To set up an IRF fabric, refer to the items in Table 10.

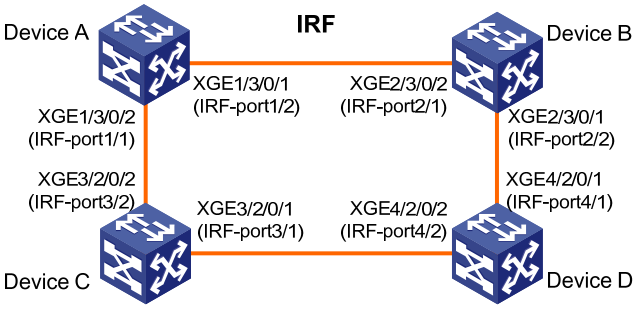
Table 10 Basic IRF setup

Item	Analysis	Choice in this example
Topology	You can use a ring or daisy chain topology for a three- or four-chassis IRF fabric. For reliability, use the ring topology as long as possible.	Ring topology (see Table 10Figure 101).
Member ID assignment	IRF member IDs must be unique.	• **Device A**—1. • **Device B**—2. • **Device C**—3. • **Device D**—4.

Item	Analysis	Choice in this example
Master device	IRF members elect a master automatically. To affect the election result, you could assign the desired chassis higher member priority.	Device A.
IRF port bindings	For two neighboring IRF members, you must connect the physical ports of IRF-port 1 on one member to the physical ports of IRF-port 2 on the other. When you bind physical ports to IRF ports, you must make sure the bindings are consistent with the physical connections. For reliability, bind multiple physical ports to an IRF port. These ports will automatically aggregate for load balancing and redundancy.	See Table 10Figure 101.

To reduce the number of reboots during IRF setup, configure IRF port bindings, member ID, and member priority on each chassis before changing their operating mode to IRF mode.

Figure 101 IRF fabric topology



NOTE:

This figure shows the port numbers in IRF mode. In IRF mode, a physical port number has four segments, with the IRF member ID as the first segment. In standalone mode, a physical port number does not include the IRF member ID.

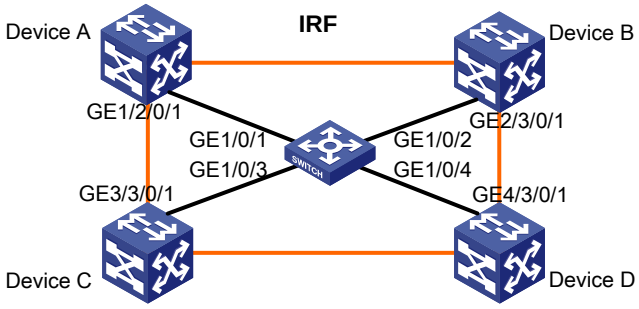
BFD MAD configuration

You can deploy BFD MAD by using one of the following methods:

- Connect all member chassis with dedicated BFD MAD links into a full mesh topology. This method is suitable for two-chassis IRF fabrics.
- Set up a dedicated BFD MAD link with an intermediate device for each IRF member chassis, as shown in Figure 102. This method is suitable for three- or four-chassis IRF fabrics, because it uses fewer physical ports than the previous method.

The intermediate device forwards BFD MAD packets transparently. The only configuration requirement for this device is that you must assign all BFD MAD links to the VLAN used for BFD MAD.

Figure 102 BFD MAD connection diagram



Software feature configuration

On the IRF fabric, you configure software features in the same way as you do with a standalone switch.

For connecting to the downstream switches and the upstream egress routers, you could set up multichassis link aggregations, as shown in Figure 103. A link aggregation could span one member chassis, some of the member chassis, or all member chassis, depending on the link redundancy requirements and number of available links.

The link aggregation mode can be dynamic or static. This example uses dynamic aggregation mode for all link aggregations.

To use the IRF fabric as the gateway for servers, you must configure VLAN interfaces for providing gateway services, as shown in Table 11.

To use the IRF fabric in a Layer 3 network, you must configure routing. In this example, OSPF is configured.

Figure 103 Connection diagram for the IRF fabric in a Layer 3 network

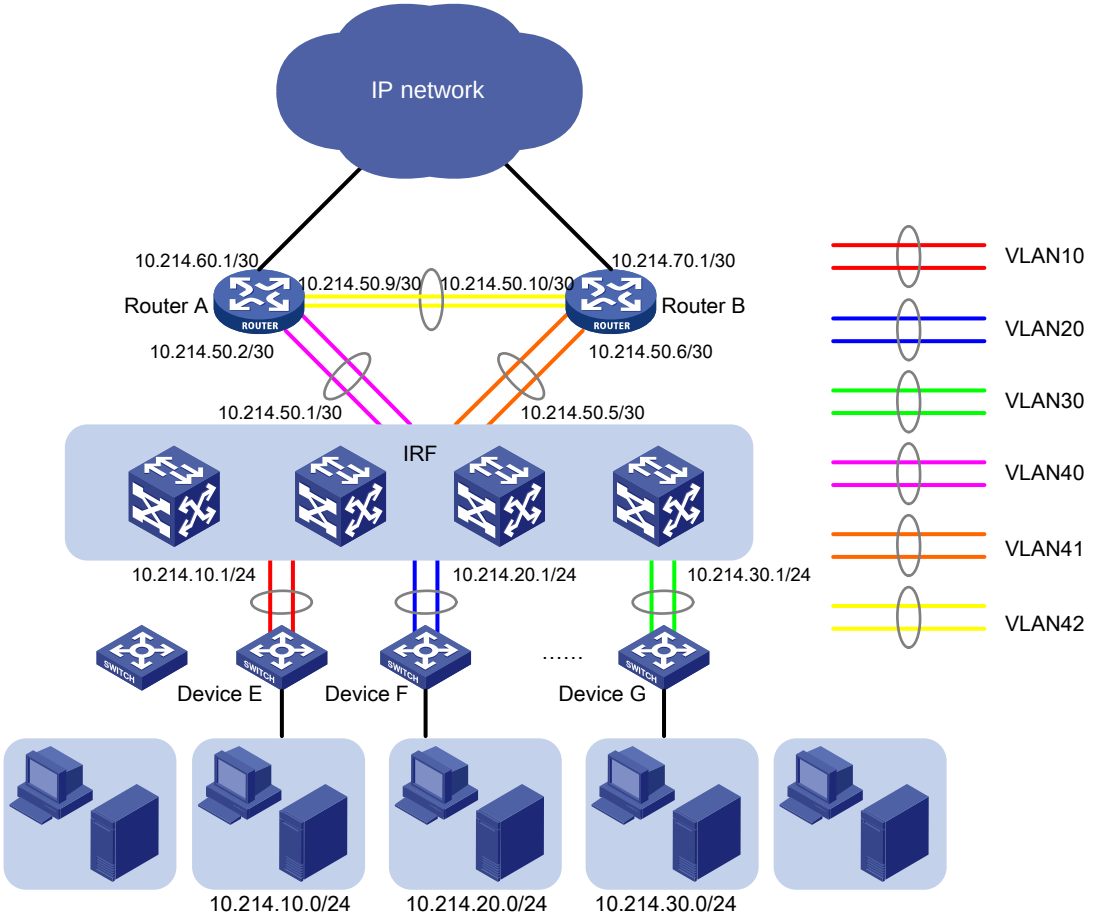


Table 11 Link aggregations and VLAN assignment scheme

Aggregate interface	Member ports	VLANs	VLAN interface's IP address
Router A:			
Bridge-Aggregation 40	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4	VLAN 40	10.214.50.2/30
Bridge-Aggregation 42	GigabitEthernet1/0/5 GigabitEthernet1/0/6	VLAN 42	10.214.50.9/30
Router B:			
Bridge-Aggregation 41	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4	VLAN 41	10.214.50.6/30
Bridge-Aggregation 42	GigabitEthernet1/0/5 GigabitEthernet1/0/6	VLAN 42	10.214.50.10/30
IRF fabric:			

Aggregate interface	Member ports	VLANs	VLAN interface's IP address
Bridge-Aggregation 10	GigabitEthernet1/4/0/10 GigabitEthernet2/4/0/10 GigabitEthernet3/4/0/10 GigabitEthernet4/4/0/10	VLAN 10	10.214.10.1/24
Bridge-Aggregation 20	GigabitEthernet1/4/0/11 GigabitEthernet2/4/0/11 GigabitEthernet3/4/0/11 GigabitEthernet4/4/0/11	VLAN 20	10.214.20.1/24
Bridge-Aggregation 30	GigabitEthernet1/4/0/12 GigabitEthernet2/4/0/12 GigabitEthernet3/4/0/12 GigabitEthernet4/4/0/12	VLAN 30	10.214.30.1/24
Bridge-Aggregation 40	GigabitEthernet1/4/0/13 GigabitEthernet2/4/0/13 GigabitEthernet3/4/0/13 GigabitEthernet4/4/0/13	VLAN 40	10.214.50.1/30
Bridge-Aggregation 41	GigabitEthernet1/4/0/14 GigabitEthernet2/4/0/14 GigabitEthernet3/4/0/14 GigabitEthernet4/4/0/14	VLAN 41	10.214.50.5/30
Device E:			
Bridge-Aggregation 10	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4	VLAN 10	No VLAN interface is required.
Device F:			
Bridge-Aggregation 20	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4	VLAN 20	No VLAN interface is required.
Device G:			
Bridge-Aggregation 30	GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/4	VLAN 30	No VLAN interface is required.

Configuration restrictions and guidelines

When you configure a BFD MAD-enabled IRF fabric, follow the restrictions and guidelines in this section.

BFD MAD

When you configure BFD MAD, follow these restrictions and guidelines:

Category	Restrictions and guidelines
VLAN	• Do not enable BFD MAD on VLAN-interface 1. • Do not use the BFD MAD VLAN for any purpose other than configuring BFD MAD. No Layer 2 or Layer 3 features, including ARP and LACP, can work on the BFD MAD-enabled VLAN interface or any port in the VLAN. If you configure any other feature on the VLAN, neither the configured feature nor the BFD MAD function can work correctly. • If an intermediate device is used, assign the ports of BFD MAD links to the BFD MAD VLAN on the device. • The IRF fabrics in a network must use different BFD MAD VLANs.
MAD IP address	• To avoid problems, only use the **mad ip address** command to configure IP addresses on the BFD MAD-enabled VLAN interface. For example, an IP address configured with the **ip address** command or a VRRP virtual IP address can cause problems. • All MAD IP addresses on the BFD MAD-enabled VLAN interface must be on the same subnet.
Feature compatibility	• Disable the spanning tree feature on any port in the BFD MAD VLAN. The MAD function is mutually exclusive with the spanning tree feature. • Do not bind a BFD MAD-enabled VLAN interface to any VPN instance. The MAD function is mutually exclusive with VPN.

IRF port binding

When you bind physical ports to an IRF ports, follow these restrictions and guidelines:

- IRF physical ports must be set to bridge mode (the default).
- When you bind physical ports to an IRF port, you must set all the physical ports to operate in the same mode: normal or enhanced. If you do not specify a mode, the normal mode applies.
- The physical ports of two connected IRF ports must operate in the same mode: normal or enhanced.
- To use the MPLS L2VPN or VPLS function in an IRF fabric, you must specify the **mode enhanced** option when binding IRF ports.

Configuration procedures

Setting up the IRF fabric

1. Configure Device A:

   # Assign member ID 1 to Device A.

   ```
   <Sysname> system-view
   [Sysname] irf member 1
    Info: Member ID change will take effect after the member reboots and operates in IRF mode.
   ```

   # Bind Ten-GigabitEthernet 3/0/2 to IRF-port 1, and bind Ten-GigabitEthernet 3/0/1 to IRF-port 2.

IMPORTANT:

To avoid traffic forwarding problems, shut down physical ports before binding them to an IRF port.

```
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 3/0/2
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 3/0/1
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
```

Assign an IRF member priority of 31 to Device A. This high priority makes sure Device A can be elected as the master.

```
[Sysname] irf priority 31
```

Save the running configuration before changing the operating mode to IRF. The mode change requires a system reboot, which can cause all unsaved settings to be lost.

```
[Sysname] quit
<Sysname> save
```

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device A reboots to form a one-chassis IRF fabric.

2. Configure Device B:

Assign member ID 2 to Device B.

```
<Sysname> system-view
[Sysname] irf member 2
```

```
 Info: Member ID change will take effect after the member reboots and operates in IRF
mode.
```

Bind Ten-GigabitEthernet 3/0/2 to IRF-port 1, and bind Ten-GigabitEthernet 3/0/1 to IRF-port2.

```
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 3/0/2
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 3/0/2
[Sysname-Ten-GigabitEthernet3/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 3/0/1
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/1] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device B to Device A, as shown in Figure 101.

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device B reboots to join the IRF fabric. A two-chassis IRF fabric is formed.

3. Configure Device C:

Assign member ID 3 to Device C.

```
<Sysname> system-view
[Sysname] irf member 3
 Info: Member ID change will take effect after the member reboots and operates in IRF
mode.
```

Bind Ten-GigabitEthernet 2/0/1 to IRF-port 1, and bind Ten-GigabitEthernet 2/0/2 to IRF-port 2.

```
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 2/0/1
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 2/0/2
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device C to Device A and Device D, as shown in Figure 101.

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device C reboots to join the IRF fabric.

4. Configure Device D:

Assign member ID 4 to Device D.

```
<Sysname> system-view
[Sysname] irf member 4
 Info: Member ID change will take effect after the member reboots and operates in IRF
mode.
```

Bind Ten-GigabitEthernet 2/0/1 to IRF-port 1, and bind Ten-GigabitEthernet 2/0/2 to IRF-port 2.

```
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
```

```
[Sysname] irf-port 1
[Sysname-irf-port1] port group interface ten-gigabitethernet 2/0/1
[Sysname-irf-port1] quit
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
[Sysname] irf-port 2
[Sysname-irf-port2] port group interface ten-gigabitethernet 2/0/2
[Sysname-irf-port2] quit
[Sysname] interface ten-gigabitethernet 2/0/2
[Sysname-Ten-GigabitEthernet2/0/2] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/2] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device D to Device B and Device C, as shown in Figure 101.

Enable IRF mode.

```
<Sysname> system-view
[Sysname] chassis convert mode irf
The device will switch to IRF mode and reboot. You are recommended to save the current
running configuration and specify the configuration file for the next startup.
Continue? [Y/N]:y
 Do you want to convert the content of the next startup configuration file
flash:/startup.cfg to make it available in IRF mode? [Y/N]:y
 Please wait...
 Saving the converted configuration file to the main board succeeded.
Slot 1:
 Saving the converted configuration file succeeded.
 Now rebooting, please wait...
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

Configuring BFD MAD on the IRF fabric

Create VLAN 3 (BFD MAD VLAN), and add all ports used for BFD MAD to the VLAN, including GigabitEthernet 1/2/0/1, GigabitEthernet 2/3/0/1, GigabitEthernet 3/3/0/1, and GigabitEthernet 4/3/0/1.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] port gigabitethernet 1/2/0/1 gigabitethernet 2/3/0/1 gigabitethernet
3/3/0/1 gigabitethernet 4/3/0/1
[Sysname-vlan3] quit
```

Create VLAN-interface 3, and configure a MAD IP address for each member chassis on the interface.

```
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad bfd enable
[Sysname-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[Sysname-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
```

```
[Sysname-Vlan-interface3] mad ip address 192.168.2.3 24 member 3
[Sysname-Vlan-interface3] mad ip address 192.168.2.4 24 member 4
[Sysname-Vlan-interface3] quit
```

Disable the spanning tree feature on the ports in the BFD MAD VLAN.

```
[Sysname] interface gigabitethernet 1/2/0/1
[Sysname-Gigabitethernet-1/2/0/1] undo stp enable
[Sysname-Gigabitethernet-1/2/0/1] quit
[Sysname] interface gigabitethernet 2/3/0/1
[Sysname-Gigabitethernet-2/3/0/1] undo stp enable
[Sysname-Gigabitethernet-2/3/0/1] quit
[Sysname] interface gigabitethernet 3/3/0/1
[Sysname-Gigabitethernet-3/3/0/1] undo stp enable
[Sysname-Gigabitethernet-3/3/0/1] quit
[Sysname] interface gigabitethernet 4/3/0/1
[Sysname-Gigabitethernet-4/3/0/1] undo stp enable
[Sysname-Gigabitethernet-4/3/0/1] quit
```

Configuring software features

The core router configuration in this example does not include the connection to the public network.

1. Configure Router A:

   # Create VLANs 40 and 42.

   ```
   <RouterA> system-view
   [RouterA] vlan 40
   [RouterA-vlan40] quit
   [RouterA] vlan 42
   [RouterA-vlan42] quit
   ```

   # Create Bridge-Aggregation 40 and set its link aggregation mode to dynamic.

   ```
   [RouterA] interface bridge-aggregation 40
   [RouterA-Bridge-Aggregation40] link-aggregation mode dynamic
   [RouterA-Bridge-Aggregation40] quit
   ```

   # Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the aggregation group for Bridge-Aggregation 40.

   ```
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] port link-aggregation group 40
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] port link-aggregation group 40
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/3
   [RouterA-GigabitEthernet1/0/3] port link-aggregation group 40
   [RouterA-GigabitEthernet1/0/3] quit
   [RouterA] interface gigabitethernet 1/0/4
   [RouterA-GigabitEthernet1/0/4] port link-aggregation group 40
   [RouterA-GigabitEthernet1/0/4] quit
   ```

   # Assign Bridge-Aggregation 40 to VLAN 40.

   ```
   [RouterA] interface bridge-aggregation 40
   [RouterA-Bridge-Aggregation40] port access vlan 40
   ```

Create Bridge-Aggregation 42 and set its link aggregation mode to dynamic.

```
[RouterA] interface bridge-aggregation 42
[RouterA-Bridge-Aggregation42] link-aggregation mode dynamic
[RouterA-Bridge-Aggregation42] quit
```

Assign GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 to the aggregation group for Bridge-Aggregation 42.

```
[RouterA] interface gigabitethernet 1/0/5
[RouterA-GigabitEthernet1/0/5] port link-aggregation group 42
[RouterA-GigabitEthernet1/0/5] quit
[RouterA] interface gigabitethernet 1/0/6
[RouterA-GigabitEthernet1/0/6] port link-aggregation group 42
[RouterA-GigabitEthernet1/0/6] quit
```

Assign Bridge-Aggregation 42 to VLAN 42.

```
[RouterA] interface bridge-aggregation 42
[RouterA-Bridge-Aggregation42] port access vlan 42
[RouterA-Bridge-Aggregation42] quit
```

Create VLAN-interface 40 and VLAN-interface 42, and assign IP addresses to them.

```
[RouterA] interface vlan-interface 40
[RouterA-Vlan-interface40] ip address 10.214.50.2 30
[RouterA-Vlan-interface40] quit
[RouterA] interface vlan-interface 42
[RouterA-Vlan-interface42] ip address 10.214.50.9 30
[RouterA-Vlan-interface42] quit
```

Configure OSPF.

```
[RouterA] ospf
[RouterA-ospf-1] import-route direct
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.214.60.0 0.0.0.3
[RouterA-ospf-1-area-0.0.0.0] network 10.214.50.0 0.0.0.3
[RouterA-ospf-1-area-0.0.0.0] network 10.214.50.8 0.0.0.3
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

2. Configure Router B:

Create VLANs 41 and 42.

```
<RouterB> system-view
[RouterB] vlan 41
[RouterB-vlan41] quit
[RouterB] vlan 42
[RouterB-vlan42] quit
```

Create Bridge-Aggregation 41 and set its link aggregation mode to dynamic.

```
[RouterB] interface bridge-aggregation 41
[RouterB-Bridge-Aggregation41] link-aggregation mode dynamic
[RouterB-Bridge-Aggregation41] quit
```

Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet1/0/3, and GigabitEthernet 1/0/4 to the aggregation group for Bridge-Aggregation 41.

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] port link-aggregation group 41
```

```
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] port link-aggregation group 41
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-GigabitEthernet1/0/3] port link-aggregation group 41
[RouterB-GigabitEthernet1/0/3] quit
[RouterB] interface gigabitethernet 1/0/4
[RouterB-GigabitEthernet1/0/4] port link-aggregation group 41
[RouterB-GigabitEthernet1/0/4] quit
```

Assign Bridge-Aggregation 41 to VLAN 41.

```
[RouterB] interface bridge-aggregation 41
[RouterB-Bridge-Aggregation41] port access vlan 41
[RouterB-Bridge-Aggregation41] quit
```

Create Bridge-Aggregation 42 and set its link aggregation mode to dynamic.

```
[RouterB] interface bridge-aggregation 42
[RouterB-Bridge-Aggregation42] link-aggregation mode dynamic
[RouterB-Bridge-Aggregation42] port access vlan 42
[RouterB-Bridge-Aggregation42] quit
```

Assign GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 to the aggregation group for Bridge-Aggregation 42.

```
[RouterB] interface gigabitethernet 1/0/5
[RouterB-GigabitEthernet1/0/5] port link-aggregation group 42
[RouterB-GigabitEthernet1/0/5] quit
[RouterB] interface gigabitethernet 1/0/6
[RouterB-GigabitEthernet1/0/6] port link-aggregation group 42
[RouterB-GigabitEthernet1/0/6] quit
```

Assign Bridge-Aggregation 42 to VLAN 42.

```
[RouterB] interface bridge-aggregation 42
[RouterB-Bridge-Aggregation42] port access vlan 42
[RouterB-Bridge-Aggregation42] quit
```

Create VLAN-interface 41 and VLAN-interface 42, and assign IP addresses to them.

```
[RouterB] interface vlan-interface 41
[RouterB-Vlan-interface41] ip address 10.214.50.6 30
[RouterB-Vlan-interface41] quit
[RouterB] interface vlan-interface 42
[RouterB-Vlan-interface42] ip address 10.214.50.10 30
[RouterB-Vlan-interface42] quit
```

Configure OSPF.

```
[RouterB] ospf
[RouterB-ospf-1] import-route direct
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.214.70.0 0.0.0.3
[RouterB-ospf-1-area-0.0.0.0] network 10.214.50.0 0.0.0.3
[RouterB-ospf-1-area-0.0.0.0] network 10.214.50.8 0.0.0.3
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

3. Configure the IRF fabric:

Create VLANs 10, 20, 30, 40, and 41.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] vlan 20
[Sysname-vlan20] quit
[Sysname] vlan 30
[Sysname-vlan30] quit
[Sysname] vlan 40
[Sysname-vlan40] quit
[Sysname] vlan 41
[Sysname-vlan41] quit
```

Create Bridge-Aggregation 10 and set its link aggregation mode to dynamic.

```
[Sysname] interface bridge-aggregation 10
[Sysname-Bridge-Aggregation10] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation10] quit
```

Assign GigabitEthernet 1/4/0/10, GigabitEthernet 2/4/0/10, GigabitEthernet 3/4/0/10, and GigabitEthernet 4/4/0/10 to the aggregation group for Bridge-Aggregation 10.

```
[Sysname] interface gigabitethernet 1/4/0/10
[Sysname-GigabitEthernet1/4/0/10] port link-aggregation group 10
[Sysname-GigabitEthernet1/4/0/10] quit
[Sysname] interface gigabitethernet 2/4/0/10
[Sysname-GigabitEthernet2/4/0/10] port link-aggregation group 10
[Sysname-GigabitEthernet2/4/0/10] quit
[Sysname] interface gigabitethernet 3/4/0/10
[Sysname-GigabitEthernet3/4/0/10] port link-aggregation group 10
[Sysname-GigabitEthernet3/4/0/10] quit
[Sysname] interface gigabitethernet 4/4/0/10
[Sysname-GigabitEthernet4/4/0/10] port link-aggregation group 10
[Sysname-GigabitEthernet4/4/0/10] quit
```

Assign Bridge-Aggregation 10 to VLAN 10.

```
[Sysname] interface bridge-aggregation 10
[Sysname-Bridge-Aggregation10] port access vlan 10
[Sysname-Bridge-Aggregation10] quit
```

Repeat the previous aggregate interface configuration steps to configure Bridge-Aggregation interfaces 20, 30, 40, and 41, in compliance with the scheme in Table 11.

Create interfaces for VLANs 10, 20, 30, 40, and 41, and assign IP addresses to the interfaces.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 10.214.10.1 24
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] ip address 10.214.20.1 24
[Sysname-Vlan-interface20] quit
[Sysname] interface vlan-interface 30
[Sysname-Vlan-interface30] ip address 10.214.30.1 24
[Sysname-Vlan-interface30] quit
```

```
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] ip address 10.214.50.1 30
[Sysname-Vlan-interface40] quit
[Sysname] interface vlan-interface 41
[Sysname-Vlan-interface41] ip address 10.214.50.5 30
[Sysname-Vlan-interface41] quit
```

Configure OSPF.

```
[Sysname] ospf
[Sysname-ospf-1] import-route direct
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 10.214.10.0 0.0.0.255
[Sysname-ospf-1-area-0.0.0.0] network 10.214.20.0 0.0.0.255
[Sysname-ospf-1-area-0.0.0.0] network 10.214.30.0 0.0.0.255
[Sysname-ospf-1-area-0.0.0.0] network 10.214.50.0 0.0.0.3
[Sysname-ospf-1-area-0.0.0.0] network 10.214.50.4 0.0.0.3
[Sysname-ospf-1-area-0.0.0.0] quit
[Sysname-ospf-1] quit
```

4. Configure Device E:

Create Bridge-Aggregation 10 and set its link aggregation mode to dynamic.

```
[DeviceE] interface bridge-aggregation 10
[DeviceE-Bridge-Aggregation10] link-aggregation mode dynamic
[DeviceE-Bridge-Aggregation10] quit
```

Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the aggregation group for Bridge-Aggregation 10.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-aggregation group 10
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-aggregation group 10
[DeviceE-GigabitEthernet1/0/2] quit
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-aggregation group 10
[DeviceE-GigabitEthernet1/0/3] quit
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] port link-aggregation group 10
[DeviceE-GigabitEthernet1/0/4] quit
```

5. Configure Device F and Device G:

Repeat the configuration procedure for Device E to configure Device F and Device G, in compliance with Table 11. (Details not shown.)

Verifying the configuration

Verify the IRF setup, multichassis link aggregations, ring topology, and BFD MAD.

Verifing the IRF setup

Execute the **display irf** command to verify that the IRF fabric has been formed.

```
[Sysname] display irf
```

```
MemberID  Slot  Role    Priority  CPU-Mac         Description
 *+1      1     Master  31        00e0-fc0f-8c02  ---
   2      4     Standby 1         00e0-fc0f-8c17  ---
   3      7     Standby 1         00e0-fc0f-8c2c  ---
   4      1     Standby 1         00e0-fc0f-8c38  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-89bb-3034
 Auto upgrade                : yes
 Mac persistent              : always
 Domain ID                   : 0
 Auto merge                  : no
```

The output shows that the IRF fabric has four member chassis.

Execute the **display irf topology** command to verify IRF fabric connectivity.

```
[Sysname] display irf topology
                            Topology Info
 ------------------------------------------------------------------------
              IRF-Port1                IRF-Port2
 MemberID    Link       neighbor      Link       neighbor    Belong To
 1           UP         3             UP         2           00e0-fc0f-8c02
 3           UP         4             UP         1           00e0-fc0f-8c02
 4           UP         2             UP         3           00e0-fc0f-8c02
 2           UP         1             UP         4           00e0-fc0f-8c02
```

The output shows that all the IRF links are in UP state. The four-chassis IRF fabric is established.

Verifying the routing configuration

Execute the **display ip routing-table** command on the IRF fabric to verify that routes can be learned correctly.

```
[Sysname] display ip routing-table
Routing Tables: Public
         Destinations : 15       Routes : 15

Destination/Mask        Proto  Pre  Cost         NextHop         Interface

10.214.10.0/24          Direct 0    0            10.214.10.1     Vlan10
10.214.10.1/32          Direct 0    0            127.0.0.1       InLoop0
10.214.20.0/24          Direct 0    0            10.214.20.1     Vlan20
10.214.20.1/32          Direct 0    0            127.0.0.1       InLoop0
10.214.30.0/24          Direct 0    0            10.214.30.1     Vlan30
10.214.30.1/32          Direct 0    0            127.0.0.1       InLoop0
10.214.50.0/30          Direct 0    0            10.214.50.1     Vlan40
10.214.50.1/32          Direct 0    0            127.0.0.1       InLoop0
10.214.50.4/30          Direct 0    0            10.214.50.5     Vlan41
10.214.50.5/32          Direct 0    0            127.0.0.1       InLoop0
10.214.50.8/30          OSPF   10   2            10.214.50.2     Vlan40
10.214.60.0/30          OSPF   10   2            10.214.50.2     Vlan40
```

```
10.214.70.0/30          OSPF   10   2           10.214.50.6     Vlan41
127.0.0.0/8             Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32            Direct 0    0           127.0.0.1       InLoop0
```

The output shows that the IRF fabric has learned routing information from the core routers correctly.

Verifying the link backup function of multichassis aggregations

Ping 10.214.50.2 (Router A) from any server.

```
C:\Users>ping 10.214.50.2 –t
```

On the IRF fabric, shut down GigabitEthernet 1/4/0/13, a member port of Bridge-Aggregation 40.

```
[Sysname] interface gigabitethernet 1/4/0/11
[Sysname-GigabitEthernet1/4/0/11] shutdown
[Sysname-GigabitEthernet1/4/0/11] quit
```

Observe the output on the configuration terminal for the server.

```
Pinging 10.214.50.2 with 32 bytes of data:

Reply from 10.214.50.2: bytes=32 time<1ms TTL=127
Reply from 10.214.50.2: bytes=32 time<1ms TTL=127
Request timed out.
Request timed out.
Reply from 10.214.50.2: bytes=32 time<1ms TTL=127
Reply from 10.214.50.2: bytes=32 time<1ms TTL=127
```

The output shows that the address can be pinged after transient traffic disruption.

Verifying link failure protection of the ring-topology

Disconnect all IRF links between two IRF member devices to verify that the IRF fabric can operate correctly as a daisy-chained fabric.

Verifying the BFD MAD configuration

Disconnect two IRF connections: one between Device A and Device B, and the other between Device C and Device D. The disconnect actions cause the IRF fabric to break down into two parts: IRF 1 (Device A and Device C) and IRF 2 (Device B and Device D).

Verify that BFD MAD detects the split and displays the following message:

```
%May  6 15:10:05:477 2010 HP MAD/1/MAD_COLLISION_DETECTED: Multi-active devices detected,
please fix it.
```

Because the master chassis in IRF 1 has a lower member ID than the master chassis in IRF 2, LACP MAD should set IRF 2 (Device B and Device D) in Recovery state.

Verify that BFD MAD shuts down all physical network ports on Device B and Device D, except for the IRF physical ports and ports configured to be excluded from the shutdown action.

Recover the IRF links, and verify that the following message is displayed:

```
%May  6 15:12:52:935 2010 HP STM/6/STM_LINK_STATUS_UP:
 IRF port 1 is up.
%May  6 15:13:02:828 2010 HP STM/4/STM_MERGE_NEED_REBOOT:
 IRF merge occurs and the IRF system needs a reboot.
```

Log in to IRF 2 to reboot the system for a merge with IRF 1. (You can log in from the console port on Device B or Device D. Alternatively, you can log in from a network port that is excluded from the shutdown action by using the **mad exclude interface** command.)

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.
.........DONE!
 This command will reboot the device. Continue? [Y/N]:y
#May  6 15:31:09:724 2010 HP DEVM/1/REBOOT:
 Reboot device by command.
%May  6 15:31:09:734 2010 HP DEVM/5/SYSTEM_REBOOT: System is rebooting now.
```

Execute the **display irf topology** command to verify that the IRF fabric is recovered.

```
<Sysname> display irf topology
                              Topology Info
-------------------------------------------------------------------------
              IRF-Port1                IRF-Port2
MemberID    Link       neighbor      Link       neighbor    Belong To
1           UP         3             UP         2           00e0-fc0f-8c0f
2           UP         1             UP         4           00e0-fc0f-8c0f
3           UP         4             UP         1           00e0-fc0f-8c0f
4           UP         2             UP         3           00e0-fc0f-8c0f
```

Configuration files

- IRF fabric:

```
#
vlan 3
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
vlan 41
#
interface Bridge-Aggregation10
 port access vlan 10
 link-aggregation mode dynamic
#
interface Bridge-Aggregation20
 port access vlan 20
 link-aggregation mode dynamic
#
interface Bridge-Aggregation30
 port access vlan 30
 link-aggregation mode dynamic
#
interface Bridge-Aggregation40
 port access vlan 40
```

```
 link-aggregation mode dynamic
#
interface Bridge-Aggregation41
 port access vlan 41
 link-aggregation mode dynamic
#
interface Vlan-interface3
 mad bfd enable
 mad ip address 192.168.2.1 255.255.255.0 member 1
 mad ip address 192.168.2.2 255.255.255.0 member 2
 mad ip address 192.168.2.3 255.255.255.0 member 3
 mad ip address 192.168.2.4 255.255.255.0 member 4
#
interface Vlan-interface10
 ip address 10.214.10.1 255.255.255.0
#
interface Vlan-interface20
 ip address 10.214.20.1 255.255.255.0
#
interface Vlan-interface30
 ip address 10.214.30.1 255.255.255.0
#
interface Vlan-interface40
 ip address 10.214.50.1 255.255.255.252
#
interface Vlan-interface41
 ip address 10.214.50.5 255.255.255.252
#
interface gigabitethernet 1/2/0/1
 port link-mode bridge
 stp disable
 port access vlan 3
#
interface gigabitethernet 1/4/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface gigabitethernet 1/4/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface gigabitethernet 1/4/0/12
 port link-mode bridge
 port access vlan 30
 port link-aggregation group 30
#
```

```
interface gigabitethernet 1/4/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 1/4/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 2/4/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface gigabitethernet 2/4/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface gigabitethernet 2/4/0/12
 port link-mode bridge
 port access vlan 30
 port link-aggregation group 30
#
interface gigabitethernet 2/4/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 2/4/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 3/4/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface gigabitethernet 3/4/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface gigabitethernet 3/4/0/12
 port link-mode bridge
 port access vlan 30
```

```
 port link-aggregation group 30
#
interface gigabitethernet 3/4/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 3/4/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 4/4/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface gigabitethernet 4/4/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface gigabitethernet 4/4/0/12
 port link-mode bridge
 port access vlan 30
 port link-aggregation group 30
#
interface gigabitethernet 4/4/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 4/4/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
ospf 1
 area 0.0.0.0
  network 10.214.10.0 0.0.0.255
  network 10.214.20.0 0.0.0.255
  network 10.214.30.0 0.0.0.255
  network 10.214.50.0 0.0.0.3
  network 10.214.50.4 0.0.0.3
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/3/0/2 mode enhanced
#
```

```
irf-port 1/2
 port group interface Ten-GigabitEthernet1/3/0/1 mode enhanced
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/3/0/2 mode enhanced
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/3/0/1 mode enhanced
#
irf-port 3/1
 port group interface Ten-GigabitEthernet3/2/0/1 mode enhanced
#
irf-port 3/2
 port group interface Ten-GigabitEthernet3/2/0/2 mode enhanced
#
irf-port 4/1
 port group interface Ten-GigabitEthernet4/2/0/1 mode enhanced
#
irf-port 4/2
 port group interface Ten-GigabitEthernet4/2/0/2 mode enhanced
```

- Device E:

```
#
interface Bridge-Aggregation10
 link-aggregation mode dynamic
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port link-aggregation group 10
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port link-aggregation group 10
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port link-aggregation group 10
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port link-aggregation group 10
```

- Device F:

```
#
interface Bridge-Aggregation20
 link-aggregation mode dynamic
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port link-aggregation group 20
```

```
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port link-aggregation group 20
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port link-aggregation group 20
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port link-aggregation group 20
```

- Device G:

```
#
interface Bridge-Aggregation30
 link-aggregation mode dynamic
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port link-aggregation group 30
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port link-aggregation group 30
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port link-aggregation group 30
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port link-aggregation group 30
```

- Router A:

```
#
vlan 40
#
vlan 42
#
interface Bridge-Aggregation40
 port access vlan 40
 link-aggregation mode dynamic
#
interface Bridge-Aggregation42
 port access vlan 42
 link-aggregation mode dynamic
#
interface Vlan-interface40
 ip address 10.214.50.2 255.255.255.252
```

```
#
interface Vlan-interface42
 ip address 10.214.50.9 255.255.255.252
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface gigabitethernet 1/0/5
 port link-mode bridge
 port access vlan 42
 port link-aggregation group 42
#
interface gigabitethernet 1/0/6
 port link-mode bridge
 port access vlan 42
 port link-aggregation group 42
#
ospf 1
 area 0.0.0.0
  network 10.214.60.0 0.0.0.3
  network 10.214.50.0 0.0.0.3
  network 10.214.50.8 0.0.0.3
```

- Router B:

```
#
vlan 41
#
vlan 42
#
interface Bridge-Aggregation41
 port access vlan 41
 link-aggregation mode dynamic
```

```
#
interface Bridge-Aggregation42
 port access vlan 42
 link-aggregation mode dynamic
#
interface Vlan-interface41
 ip address 10.214.50.6 255.255.255.252
#
interface Vlan-interface42
 ip address 10.214.50.10 255.255.255.252
#
interface gigabitethernet 1/0/1
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 1/0/2
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 1/0/3
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 1/0/4
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface gigabitethernet 1/0/5
 port link-mode bridge
 port access vlan 42
 port link-aggregation group 42
#
interface gigabitethernet 1/0/6
 port link-mode bridge
 port access vlan 42
 port link-aggregation group 42
#
ospf 1
 area 0.0.0.0
  network 10.214.70.0 0.0.0.3
  network 10.214.50.0 0.0.0.3
  network 10.214.50.8 0.0.0.3
```

Link aggregation configuration examples

This chapter provides link aggregation configuration examples.

Example: Configuring Layer 2 link aggregation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

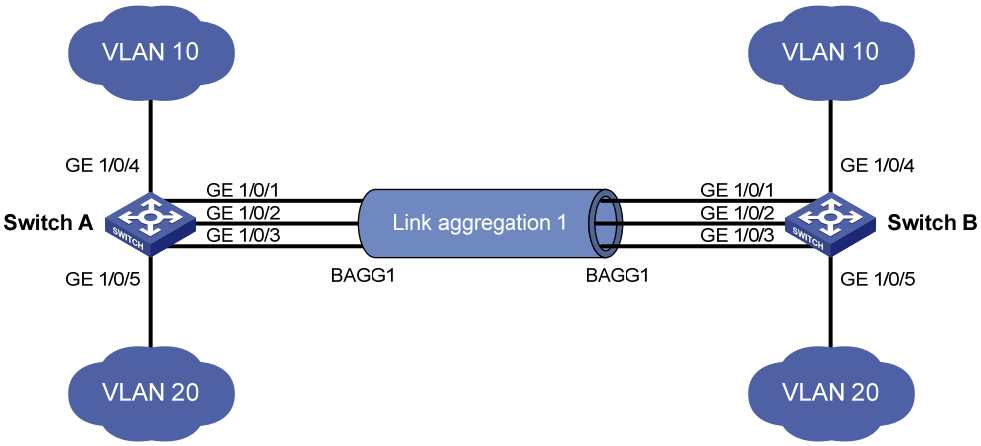
Network requirements

As shown in Figure 104, both Switch A and Switch B forward traffic from VLAN 10 and VLAN 20.

Configure link aggregation on Switch A and Switch B to meet the following requirements:

- Traffic from VLAN 10 and VLAN 20 can pass through the link aggregation.
- The member links are load shared by source and destination MAC addresses.

Figure 104 Network diagram



Requirements analysis

For traffic from VLAN 10 and VLAN 20 to pass through, configure the link type of Layer 2 aggregate interface 1 as trunk, and assign the interface to VLAN 10 and VLAN 20.

You can configure the load sharing mode for the aggregation in system view or aggregate interface view. In system view, the load sharing mode applies to all aggregations globally. In interface view, the load sharing mode applies only to the aggregate interface. Interface-specific mode has higher priority over the global mode. In this example, the global mode is used.

Configuration restrictions and guidelines

When you configure Layer 2 link aggregation, follow these restrictions and guidelines:

- When you configure an aggregation group member port, the recommended configuration procedure is as follows:
  a. Use the **display this** command in port view to check for class-two configurations (including the port isolation configuration, QinQ configuration, VLAN configuration, and MAC address learning configuration).
  b. If any class-two configurations exist, use the **undo** forms of the commands to restore the default class-two configurations.
  c. Assign the port to an aggregation group.
- Use dynamic aggregation instead of static aggregation as long as possible. In a static aggregation, peer ports cannot sense the state and availability of each other. As a result, their Selected state might differ.
- You cannot assign a port to a Layer 2 aggregation group if the port has any of the following features:
  - **Security features**—802.1X, IP source guard, MAC authentication, port security, and source interface of a portal-free rule.
  - **High availability features**—RRPP.
- Only ports operating in bridge mode can be assigned to a Layer 2 link aggregation group.

Configuration procedures

Configuring Switch A

Enter system view, and configure the link aggregation load sharing mode as source MAC address and destination MAC address.

```
<SwitchA> system-view
[SwitchA] link-aggregation load-sharing mode source-mac destination-mac
```

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

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/4
[SwitchA-vlan10] quit
```

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

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

Use one of the following methods to configure Bridge-Aggregation 1 (a Layer 2 aggregate interface):

- Create Bridge-Aggregation 1 and set its aggregation mode to static (the default).

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

- Create Bridge-Aggregation 1 and set its aggregation mode to dynamic.

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

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

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

Configure Layer 2 aggregate interface 1 as a trunk port.

```
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] port link-type trunk
```

Assign the aggregate interface to VLANs 10 and 20.

```
[SwitchA-Bridge-Aggregation1] port trunk permit vlan 10 20
 Please wait... Done.
 Configuring GigabitEthernet 1/0/1... Done.
 Configuring GigabitEthernet 1/0/2... Done.
 Configuring GigabitEthernet 1/0/3... Done.
[SwitchA-Bridge-Aggregation1] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Verify the link aggregation configuration:

- Link aggregation information when the static aggregation mode is used:

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

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

  The output shows that all member ports in the local aggregation group are Selected. The Selected states of the local member ports are not affected by the Selected states of the peer member ports.

- Link aggregation configuration when the dynamic aggregation mode is used:

```
[SwitchA]display link-aggregation verbose
```

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

Aggregation Interface: Bridge-Aggregation11
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e234-5678
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1         {ACDEF}
  GE1/0/2          S       32768    1         {ACDEF}
  GE1/0/3          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          14      32768    1         0x8000, 0000-fc00-7506 {ACDEF}
  GE1/0/2          15      32768    1         0x8000, 0000-fc00-7506 {ACDEF}
  GE1/0/3          16      32768    1         0x8000, 0000-fc00-7506 {ACDEF}
```

The output shows that the local member ports and their peer member ports are all Selected. In a dynamic link aggregation, the peer devices exchange LACPDUs to ensure port state consistency.

Configuration files

- Switch A (for static aggregation):

```
#
link-aggregation load-sharing mode source-mac destination-mac
#
vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 20
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
```

```
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
```

- Switch A (for dynamic aggregation):

```
#
link-aggregation load-sharing mode source-mac destination-mac
#
vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 20
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 10 20
link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
```

```
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
```

Example: Configuring Layer 2 link aggregation load sharing

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

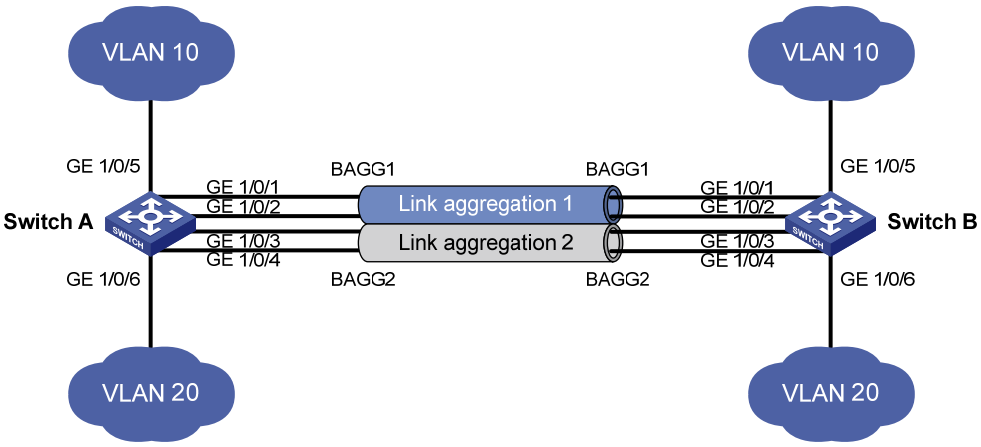
Network requirements

As shown in Figure 105, both Switch A and Switch B forward traffic from VLAN 10 and VLAN 20.

Configure link aggregation on Switch A and Switch B to meet the following requirements:

- Traffic from VLAN 10 and VLAN 20 can pass through the link aggregation.
- The member links are load shared by source MAC address for VLAN 10. The member links are load shared by destination MAC address for VLAN 20.

Figure 105 Network diagram



Requirements analysis

To configure different load sharing modes for packets in different link aggregation groups, you must configure link aggregation load sharing mode in Layer 2 aggregate interface view.

For packets from VLAN 10 to pass through aggregate interface 1, you must assign aggregate interface 1 to VLAN 10. For packets from VLAN 20 to pass through aggregate interface 2, you must assign aggregate interface 2 to VLAN 20.

Configuration restrictions and guidelines

When you configure Layer 2 load sharing, follow these restrictions and guidelines:

- When you configure an aggregation group member port, the recommended configuration procedure is as follows:
  a. Use the **display this** command in port view to check for class-two configurations (including the port isolation configuration, QinQ configuration, VLAN configuration, and MAC address learning configuration).
  b. If any class-two configurations exist, use the **undo** forms of the commands to restore the default class-two configurations.
  c. Assign the port to an aggregation group.
- You cannot assign a port to a Layer 2 aggregation group if the port has any of the following features:
  - **Security features**—802.1X, IP source guard, MAC authentication, port security, and source interface of a portal-free rule.
  - **High availability features**—RRPP.
- Only ports operating in bridge mode can be assigned to a Layer 2 link aggregation group.

Configuration procedures

Configuring Switch A

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

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

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

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/6
[SwitchA-vlan20] quit
```

Create Layer 2 aggregate interface 1.

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

Configure the link aggregation load sharing mode as source MAC address for the aggregation group 1.

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

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

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet 1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet 1/0/1] quit
```

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet 1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet 1/0/2] quit
```

Assign Layer 2 aggregate interface 1 to VLAN 10.

```
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] port access vlan 10
[SwitchA-Bridge-Aggregation1] quit
```

Create Layer 2 aggregate interface 2.

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

Configure the link aggregation load sharing mode as destination MAC address for the aggregation group 2.

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

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

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

Assign Layer 2 aggregate interface 2 to VLAN 20.

```
[SwitchA] interface bridge-aggregation 2
[SwitchA-Bridge-Aggregation2] port access vlan 20
[SwitchA-Bridge-Aggregation2] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Verify the link aggregation configuration.

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

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority  Oper-Key
--------------------------------------------------------------------------------
  GE1/2/0/21       S       32768     1
  GE1/2/0/22       S       32768     1

Aggregation Interface: Bridge-Aggregation2
```

```
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority  Oper-Key
--------------------------------------------------------------------------------
  GE1/2/0/23       S       32768     2
  GE1/2/0/24       S       32768     2
```

The output shows the following:

- Layer 2 aggregate interfaces Bridge-aggregation 1 and Bridge-aggregation 2 use the static aggregation mode.
- Each aggregation group has two Selected member ports for forwarding traffic.

Verify the load sharing mode configuration.

```
[SwitchA]display link-aggregation load-sharing mode interface Bridge-Aggregation 1
Bridge-Aggregation1 Load-Sharing Mode:
  source-mac address
[SwitchA]display link-aggregation load-sharing mode interface Bridge-Aggregation 2
Bridge-Aggregation2 Load-Sharing Mode:
  destination-mac address
```

The output shows the following:

- The link aggregation load sharing mode for Layer 2 aggregate interface 1 is source MAC address.
- The link aggregation load sharing mode for Layer 2 aggregate interface 2 is destination MAC address.

Configuration files

- Switch A:

```
#
vlan 10
#
interface GigabitEthernet1/0/5
port link-mode bridge
port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/6
port link-mode bridge
port access vlan 10
#
interface Bridge-Aggregation1
port access vlan 10
link-aggregation load-sharing mode source-mac
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 10
port link-aggregation group 1
#
```

```
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 10
port link-aggregation group 1
#
interface Bridge-Aggregation2
port access vlan 20
link-aggregation load-sharing mode destination-mac
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 20
port link-aggregation group 2
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 20
port link-aggregation group 2
```

Example: Configuring Layer 3 link aggregation

Applicable product matrix

Product series	Software Version
HP 7500	Release series 6700

Network requirements

Configure link aggregation and load sharing on Switch A and Switch B in the network shown in Figure 106 to meet the following requirements:

- Ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and Switch B preferentially become Selected ports.
- The packets between Switch A and Switch B are load-shared across only two member ports of the link aggregation group.
- The member links are load shared by source and destination IP addresses.

Figure 106 Network diagram

Requirements analysis

For GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and Switch B to preferentially become Selected ports, assign higher aggregation priorities to the two ports. By default, the aggregation

priority of a port is 32768. A smaller *port-priority* value in the **link-aggregation port-priority** *port-priority* command indicates a higher priority.

To load share packets across only two Selected ports of the link aggregation group, use the **link-aggregation selected-port maximum** command to configure the maximum number of Selected ports allowed in the aggregation group as 2.

The devices do not support configuring load sharing mode in Layer 3 aggregate interface view. To configure the link aggregation load sharing for the Layer 3 aggregation group, you must configure the load sharing mode in system view.

Configuration restrictions and guidelines

When you configure Layer 3 link aggregation, follow these restrictions and guidelines:

- By default, all Ethernet ports are operating in bridge mode as Layer 2 Ethernet ports. To assign an Ethernet port to a Layer 3 aggregation group, first use the **port link-mode route** command to configure the Ethernet port to operate in route mode as a Layer 3 Ethernet port.
- You cannot assign a port to a Layer 3 aggregation group if the port has any of the following features:
  - **IP services features**—BOOTP client, DHCP client, and IP address.
  - **High availability features**—VRRP.
  - **Security features**—Portal.
- Executing the **link-aggregation selected-port maximum** command might cause some Selected ports in an aggregation group to be Unselected.

Configuration procedures

Configuring Switch A

Enter system view, and configure the global link aggregation load sharing mode as source IP address and destination IP address.

```
<SwitchA> system-view
[SwitchA] link-aggregation load-sharing mode source-ip destination-ip
```

Use one of the following methods to configure Route-Aggregation 1 (a Layer 3 aggregate interface).

- Create Route-Aggregation 1 and set its aggregation mode to static (the default).

  ```
  [SwitchA] interface route-aggregation 1
  ```

- Create Route-Aggregation 1 and set its aggregation mode to dynamic.

  ```
  [SwitchA] interface route-aggregation 1
  [SwitchA-Route-Aggregation1] link-aggregation mode dynamic
  ```

Assign an IP address 10.1.1.1 with a subnet mask 255.255.255.0 to Layer 3 aggregate interface 1.

```
[SwitchA-Route-Aggregation1] ip address 10.1.1.1 24
```

Configure the maximum number of Selected ports allowed in the aggregation group as 2.

```
[SwitchA-Route-Aggregation1] link-aggregation selected-port maximum 2
[SwitchA-Route-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1. Configure the aggregation priority as 100 for GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-mode route
```

```
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-mode route
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] link-aggregation port-priority 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-mode route
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/3] link-aggregation port-priority 100
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Verify the link aggregation configuration.

- Link aggregation information when the static aggregation mode is used:

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

Aggregation Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority  Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          U       32768     1
  GE1/0/2          S       100       1
  GE1/0/3          S       100       1
```

- Link aggregation information when the dynamic aggregation mode is used:

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

Aggregation Interface: Route-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 0000-fc00-7506
Local:
```

```
  Port            Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1         U       32768    1         {AC}
  GE1/0/2         S       100      1         {ACDEF}
  GE1/0/3         S       100      1         {ACDEF}
Remote:
  Actor           Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1         122     32768    1         0x8000, 000f-e234-5678 {ACD}
  GE1/0/2         123     100      1         0x8000, 000f-e234-5678 {ACDEF}
  GE1/0/3         124     100      1         0x8000, 000f-e234-5678 {ACDEF}
```

The output shows that only two ports in static aggregation group 1 can be Selected ports because the maximum number of Selected ports is limited. Because the aggregation priority of GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 is higher than that of GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 become Selected ports, and GigabitEthernet 1/0/1 becomes an Unselected port.

Configuration files

- Switch A (for static aggregation):

```
#
 link-aggregation load-sharing mode destination-ip source-ip
#
interface Route-Aggregation1
 link-aggregation selected-port maximum 2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 link-aggregation port-priority 100
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 link-aggregation port-priority 100
 port link-aggregation group 1
```

- Switch A (for dynamic aggregation):

```
#
 link-aggregation load-sharing mode destination-ip source-ip
#
interface Route-Aggregation1
 link-aggregation mode dynamic
 link-aggregation selected-port maximum 2
 ip address 192.168.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
 port link-mode route
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 link-aggregation port-priority 100
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 link-aggregation port-priority 100
 port link-aggregation group 1
```

LLDP configuration examples

This chapter provides LLDP configuration examples.

Example: Configuring basic LLDP

Applicable product matrix

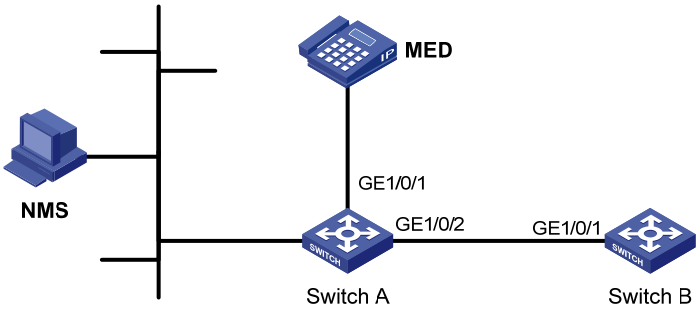
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 107, the NMS and Switch A are located in the same Ethernet network.

Enable LLDP globally on Switch A and Switch B to monitor the link between Switch A and Switch B and the link between Switch A and the MED device on the NMS.

Figure 107 Network diagram



Configuration restrictions and guidelines

To view log information about neighbor changes on the terminal screen, make sure the following features are enabled:

- Use the **terminal monitor** command to enable system information monitoring on the current terminal. By default, this feature is disabled.
- Use the **terminal logging** command to enable displaying log information on the current terminal. By default, this feature is enabled.
- Use the **info-center enable** command to enable the information center. By default, this feature is enabled.

For more information about these commands, see *Network Management and Monitoring Configuration Guide* in *HP 7500 Series Switches Configuration Guides*.

Configuration procedures

1. Configure Switch A:

   # Enable LLDP globally.

   ```
   <SwitchA> system-view
   [SwitchA] lldp enable
   ```

   # On GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, enable LLDP and set the LLDP operating mode to Rx. (By default, LLDP is enabled.)

   ```
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] lldp enable
   [SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
   [SwitchA-GigabitEthernet1/0/1] quit
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] lldp enable
   [SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
   [SwitchA-GigabitEthernet1/0/2] quit
   ```

2. Configure Switch B:

   # Enable LLDP globally.

   ```
   <SwitchB> system-view
   [SwitchB] lldp enable
   ```

   # On GigabitEthernet 1/0/1, enable LLDP and set the LLDP operating mode to Tx. (By default, LLDP is enabled.)

   ```
   [SwitchB] interface gigabitethernet 1/0/1
   [SwitchB-GigabitEthernet1/0/1] lldp enable
   [SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
   [SwitchB-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Display the global LLDP status and the LLDP status information of all ports on Switch A.

```
[SwitchA] display lldp status
Global status of LLDP : Enable
The current number of LLDP neighbors : 2
The current number of CDP neighbors : 0
LLDP neighbor information last changed time: 0 days,0 hours,4 minutes,40 seconds
Transmit interval              : 30s
Hold multiplier                : 4
Reinit delay                   : 2s
Transmit delay                 : 2s
Trap interval                  : 5s
Fast start times               : 3

Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
```

```
Roll time                       : 0s

Number of neighbors             : 1
Number of MED neighbors         : 1
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV  : 0

Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
Roll time                       : 0s

Number of neighbors             : 1
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV  : 3
```

The output shows that:

- GigabitEthernet 1/0/1 of Switch A connects to an MED device.
- GigabitEthernet 1/0/2 of Switch A connects to a non-MED device.
- Both ports are operating in Rx mode.
- They can receive LLDPDUs, but they cannot send LLDPDUs.

Remove the link between Switch A and Switch B, and display the global LLDP status and port LLDP status on Switch A.

```
[SwitchA] display lldp status
Global status of LLDP : Enable
The current number of LLDP neighbors : 1
The current number of CDP neighbors : 0
LLDP neighbor information last changed time: 0 days,0 hours,5 minutes,20 seconds
Transmit interval               : 30s
Hold multiplier                 : 4
Reinit delay                    : 2s
Transmit delay                  : 2s
Trap interval                   : 5s
Fast start times                : 3

Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
Roll time                       : 0s

Number of neighbors              : 1
Number of MED neighbors          : 1
Number of CDP neighbors          : 0
```

```
Number of sent optional TLV      : 0
Number of received unknown TLV   : 5

Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP              : Enable
Admin status                     : Rx_Only
Trap flag                        : No
Roll time                        : 0s

Number of neighbors              : 0
Number of MED neighbors          : 0
Number of CDP neighbors          : 0
Number of sent optional TLV      : 0
Number of received unknown TLV   : 0
```

The output shows that GigabitEthernet 1/0/2 of Switch A is not connected to any neighboring devices.

Configuration files

- Switch A:

```
#
lldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 lldp admin-status rx
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 lldp admin-status rx
```

- Switch B:

```
#
lldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 lldp admin-status tx
```

Example: Configuring CDP-compatible LLDP

Applicable product matrix

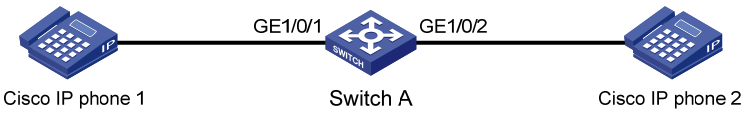
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 108, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A are both connected to a Cisco IP phone, which sends tagged voice traffic.

Configure voice VLAN 2 on Switch A. Enable CDP compatibility for LLDP on Switch A to allow the Cisco IP phones to automatically configure the voice VLAN for their voice traffic.

Figure 108 Network diagram



Configuration restrictions and guidelines

When you configure CDP-compatible LLDP, follow these guidelines:

- To make CDP-compatible LLDP take effect on a port, you must enable CDP-compatible LLDP globally and configure the operating mode of CDP-compatible LLDP on the port as TxRx.
- The maximum TTL value that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, make sure the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds.
- Only Release 6700 supports including IP addresses in outgoing CDP packets and displaying IP addresses of CDP neighbors.

Configuration procedures

1. Configure a voice VLAN on Switch A:

   # Create VLAN 2.

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

   # Set the link type of GigabitEthernet 1/0/1 to trunk.

   ```
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-type trunk
   ```

   # Enable voice VLAN on GigabitEthernet 1/0/1.

   ```
   [SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
   [SwitchA-GigabitEthernet1/0/1] quit
   ```

   # Set the link type of GigabitEthernet 1/0/2 to trunk.

   ```
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] port link-type trunk
   ```

   # Enable voice VLAN on GigabitEthernet 1/0/2.

   ```
   [SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
   [SwitchA-GigabitEthernet1/0/2] quit
   ```

2. Configure CDP-compatible LLDP on Switch A:

   # Enable both LLDP and CDP-compatible LLDP globally.

```
[SwitchA] lldp enable
[SwitchA] lldp compliance cdp
```

Enable LLDP on GigabitEthernet 1/0/1. This step is optional, because LLDP is enabled on ports by default.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

Configure LLDP to operate in TxRx mode on GigabitEthernet 1/0/1. This step is optional, because the default LLDP operating mode is TxRx.

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx
```

Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit
```

Enable LLDP on GigabitEthernet 1/0/2. This step is optional, because LLDP is enabled on ports by default.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

Configure LLDP to operate in TxRx mode on GigabitEthernet 1/0/2. This step is optional, because the default LLDP operating mode is TxRx.

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx
```

Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display the neighbor information on Switch A.

```
[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  CDP neighbor index : 1
  Chassis ID         : SEP00141CBCDBFE
  Address            : 192.168.1.55
  Port ID            : Port 1
  Software version   : P0030301MFG2
  Platform           : Cisco IP Phone 7960
  Duplex             : Full

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
  CDP neighbor index : 2
  Chassis ID         : SEP00141CBCDBFF
  Address            : 192.168.1.56
  Port ID            : Port 1
  Sofrware version   : P0030301MFG2
  Platform           : Cisco IP Phone 7960
  Duplex             : Full
```

The sample output shows that:

- Switch A has discovered the IP phones connected to GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
- Switch A has obtained the device information of these IP phones.

Configuration files

```
#
 lldp enable
 lldp compliance cdp
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1
 voice vlan 2 enable
 lldp compliance admin-status cdp txrx
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1
 voice vlan 2 enable
 lldp compliance admin-status cdp txrx
#
```

MAC address table configuration examples

This chapter provides typical application scenarios and configuration examples for static MAC address entries, dynamic MAC address entries, and blackhole MAC address entries.

Example: Configuring the MAC address table

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620
	Release series 6630
	Release series 6700

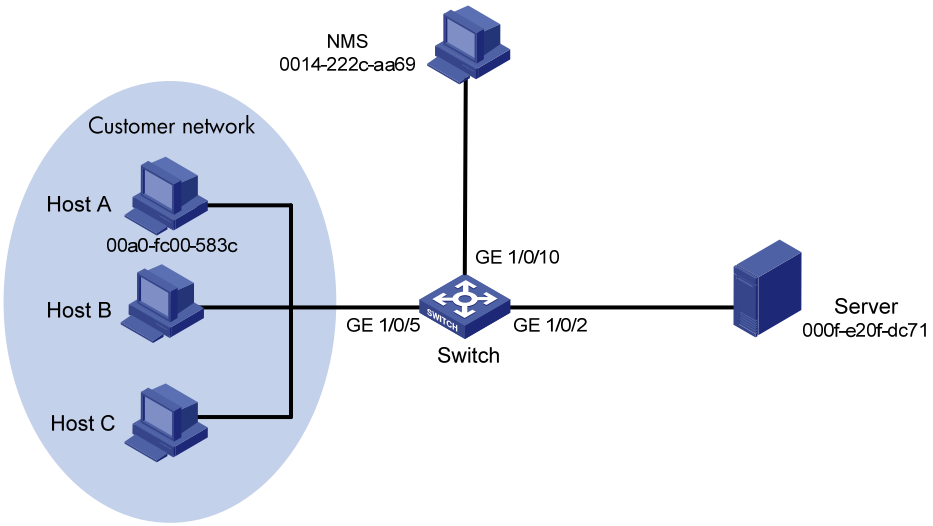
Network requirements

As shown in Figure 109, the server, NMS, and the customer network forward traffic in VLAN 10.

Configure the MAC address table to meet the following requirements:

- The switch uses a static MAC address entry to only unicast the frames destined for the server.
- The switch uses a static MAC address entry to forward frames destined for the NMS.
- The interface connecting to the NMS provides access for only the NMS.
- The interface connecting to the customer network generates MAC address entries by learning source MAC addresses of incoming frames.
- The switch does not forward frames sourced from the host (Host A in this example) which launches attacks.

Figure 109 Network diagram



Requirements analysis

To allow the interface connecting to the NMS to provide access for only the NMS, set the MAC address learning limit to 0 on GigabitEthernet 1/0/10. As a result, the switch forwards only frames sourced from the NMS, and other hosts cannot communicate through the interface.

To prevent the switch from being attacked by a large amount of frames with different source MAC addresses from Host A, disable MAC address learning on GigabitEthernet 1/0/5.

Configuration restrictions and guidelines

The switch discards frames whose source or destination MAC address matches a blackhole MAC address entry.

Configuration procedures

Create VLAN 10, and assign interfaces GigabitEthernet 1/0/2, GigabitEthernet 1/0/5, and GigabitEthernet 1/0/10 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port GigabitEthernet1/0/2 GigabitEthernet1/0/5 GigabitEthernet1/0/10
[Switch-vlan10] quit
```

Create a static MAC address entry for the server MAC address on GigabitEthernet 1/0/2.

```
[Switch] mac-address static 000f-e20f-dc71 interface GigabitEthernet 1/0/2 vlan 10
```

Set the MAC address learning limit to 0 on GigabitEthernet 1/0/10.

```
[Switch] interface GigabitEthernet 1/0/10
[Switch-GigabitEthernet1/0/10] mac-address max-mac-count 0
```

Configure a static MAC address entry for the NMS MAC address on the interface.

```
[Switch-GigabitEthernet1/0/10] mac-address static 0014-222c-aa69 vlan 10
```

Disable MAC address learning on GigabitEthernet 1/0/5 when attacks are found on the interface. Disabling MAC address learning can result in broadcast storms. To limit the size of broadcast traffic, set the broadcast suppression threshold as 50% of the maximum interface rate.

```
[Switch] interface GigabitEthernet 1/0/5
[Switch-GigabitEthernet1/0/5] mac-address mac-learning disable
[Switch-GigabitEthernet1/0/5] broadcast-suppression 50
[Switch-GigabitEthernet1/0/5] quit
```

After locating the attack source Host A, configure a blackhole MAC address entry for the Host A MAC address.

```
[Switch] mac-address blackhole 00a0-fc00-583c vlan 10
```

Enable MAC address learning on GigabitEthernet 1/0/5. Otherwise, broadcast storms might occur.

```
[Switch] interface GigabitEthernet 1/0/5
[Switch-GigabitEthernet1/0/5] undo mac-address mac-learning disable
```

Disable broadcast suppression on GigabitEthernet 1/0/5.

```
[Switch-GigabitEthernet1/0/5] undo broadcast-suppression
[Switch-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Display the MAC address table configuration.

```
[Switch] display mac-address
MAC ADDR          VLAN ID   STATE            PORT INDEX              AGING TIME(s)
00a0-fc00-583c    10        Blackhole        N/A                     NOAGED
000f-e20f-dc71    10        Config static    GigabitEthernet1/0/2    NOAGED
0014-222c-aa69    10        Config static    GigabitEthernet1/0/10   NOAGED
00e0-fc5e-b1fb    10        Learned          GigabitEthernet1/0/5    AGING
00e0-fc55-f116    10        Learned          GigabitEthernet1/0/5    AGING
0000-fc00-7507    10        Learned          GigabitEthernet1/0/5    AGING
0023-8927-aff0    10        Learned          GigabitEthernet1/0/5    AGING
0023-8927-b003    10        Learned          GigabitEthernet1/0/5    AGING
  ---  8 mac address(es) found  ---
```

Configuration files

```
#
vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 mac-address static 000f-e20f-dc71 vlan 10
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 10
 mac-address max-mac-count 0
 mac-address static 0014-222c-aa69 vlan 10
#
 mac-address blackhole 00a0-fc00-583c vlan 10
#
```

Example: Configuring MAC Information

Applicable product matrix

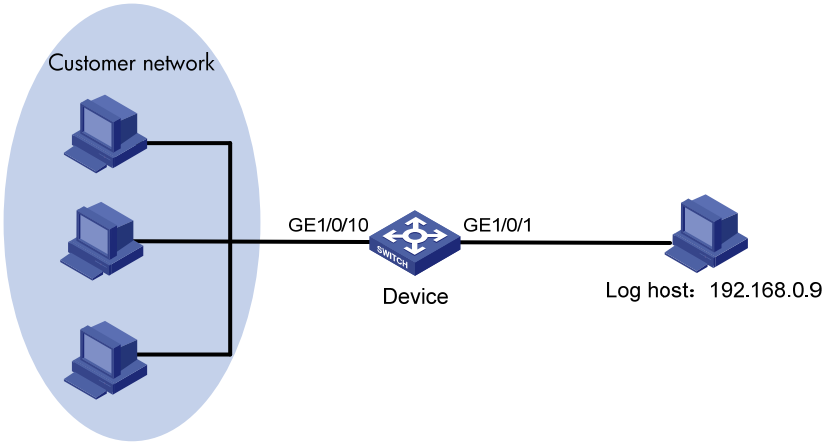
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 110, configure MAC Information to meet the following requirements:

- The device sends MAC address changes in syslog messages to the log host.
- Syslog messages are not sent frequently.

Figure 110 Network diagram



Requirements analysis

To prevent syslog messages from being sent frequently, set the interval for sending syslog messages to a value longer than the default.

Configuration restrictions and guidelines

When you configure MAC Information, follow these restrictions and guidelines:

- To use MAC Information correctly on an interface, you must enable MAC Information globally and on the interface.
- For an HP 7500 switch, MAC Information is not applicable to SD and EB cards that are operating in MAC extension mode (**bridging**) or mixed extension mode (**mix-bridging-routing**).
- The device records and sends the following MAC addresses:
  - MAC addresses that are dynamically learned.

    - MAC addresses that pass MAC address authentication.
    - MAC addresses that pass 802.1X authentication.
    - MAC addresses that match the OUI addresses for voice VLANs.
    - Secure MAC addresses.
- The device does not record or send following MAC addresses:
    - Blackhole MAC addresses.
    - Static MAC addresses.
    - Manually configured dynamic MAC addresses.
    - Multicast MAC addresses.
    - The local MAC address.
- Before configuring the device to send syslog messages to the log host, make sure the device and the log host can reach each other.

Configuration procedures

1. Configure MAC Information:

   # Enable MAC Information globally.

   ```
   <Device> system-view
   [Device] mac-address information enable
   ```

   # Configure the MAC Information mode as syslog.

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

   # Enable MAC Information on GigabitEthernet 1/0/10.

   ```
   [Device] interface gigabitethernet 1/0/10
   [Device-GigabitEthernet1/0/10] mac-address information enable added
   [Device-GigabitEthernet1/0/10] mac-address information enable deleted
   [Device-GigabitEthernet1/0/10] quit
   ```

   # Set the interval for sending syslog messages to 300 seconds.

   ```
   [Device] mac-address information interval 300
   ```

2. Configure the device to send syslog messages to the log host:

   # Enable the information center.

   ```
   [Device] info-center enable
   ```

   # Configure the log host address.

   ```
   [Device] info-center loghost 192.168.0.9
   ```

   # Enable the information center to send the MAC module's information with a severity level of at least informational to the log host.

   ```
   [Device] info-center source mac channel loghost log level informational state on
   ```

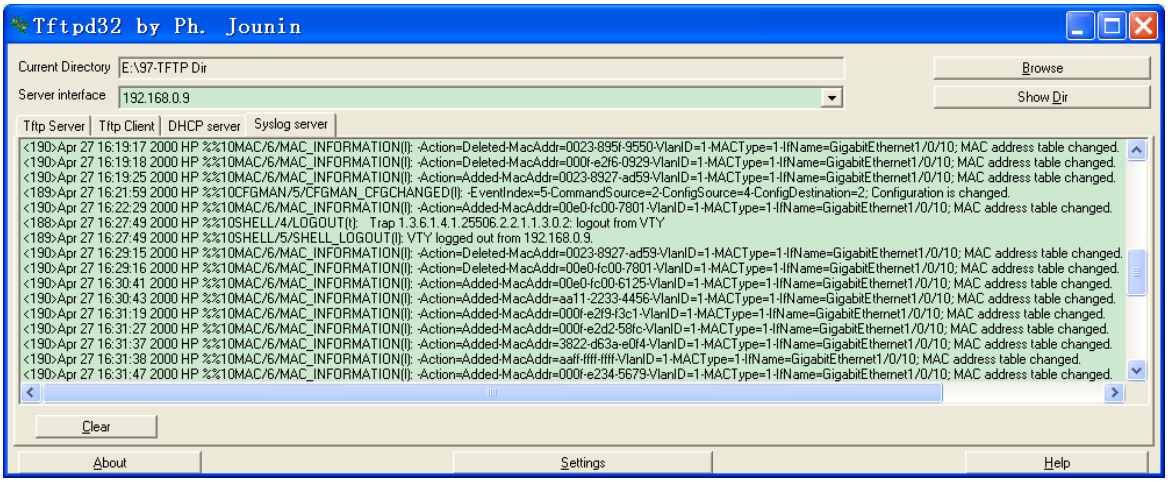
3. Run available applications that can receive log information on the log host.

Verifying the configuration

Display MAC Information messages on the log host to verify the configuration.

This example uses the **tftpd32** log host software. Figure 111 shows the sample messages received by the tool.

Figure 111 Log information



Configuration files

```
#
 mac-address information enable
 mac-address information interval 300
 mac-address information mode syslog
#
 info-center enable
 info-center source mac channel loghost log level informational state on
 info-center loghost 192.168.0.9
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 mac-address information enable added
 mac-address information enable deleted
#
```

MAC authentication configuration examples

This chapter provides examples for configuring MAC authentication to control network access of users.

General restrictions and guidelines

MAC authentication is mutually exclusive with link aggregation and service loopback groups.

Example: Configuring local MAC authentication

Applicable product matrix

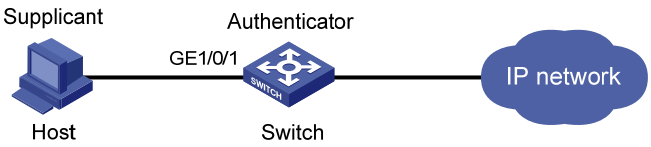
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 112:

- Configure local MAC authentication on the switch to control the network access of users.
- Use the MAC address of each user as the username and password for authentication, and the MAC addresses are hyphenated and in lower case.

Figure 112 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

Configuration restrictions and guidelines

When you configure local MAC authentication, follow these restrictions and guidelines:

- When you create a local user account, make sure the account uses the same format as the one configured by the **mac-authentication user-name-format** command.

- Enable MAC authentication globally only after you have configured the authentication-related parameters. Otherwise, users might fail to pass local MAC authentication.

Configuration procedures

Create a local user account. Both of the username and password are the host's MAC address, and the service type is LAN access.

```
<Switch> system-view
[Switch] local-user 68-05-ca-06-55-7b
[Switch-luser-68-05-ca-06-55-7b] password simple 68-05-ca-06-55-7b
[Switch-luser-68-05-ca-06-55-7b] service-type lan-access
[Switch-luser-68-05-ca-06-55-7b] quit
```

Configure ISP domain **aabbcc.net** to perform local authentication for LAN access users.

```
[Switch] domain aabbcc.net
[Switch-isp-aabbcc.net] authentication lan-access local
[Switch-isp-aabbcc.net] quit
```

Specify the ISP domain for MAC authentication.

```
[Switch] mac-authentication domain aabbcc.net
```

Set the MAC authentication offline detect timer and quiet timer. The switch detects whether a user has gone offline every 180 seconds. If a user fails MAC authentication, the switch does not authenticate the user within 180 seconds.

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

Configure MAC authentication to use MAC-based accounts. The MAC address usernames and passwords are hyphenated and in lower case.

```
[Switch] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication on port GigabitEthernet 1/0/1.

```
[Switch] mac-authentication interface gigabitethernet 1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Enable MAC authentication globally.

```
[Switch] mac-authentication
 Mac-auth is enabled globally.
```

Verifying the configuration

Display MAC authentication settings and statistics.

```
<Switch> display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 180s
          Quiet period is 180s
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 1
          Current domain is aabbcc.net
```

```
Silent MAC User info:
          MAC Addr         From Port                    Port Index


GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 364
  Max number of on-line users is 1
  Current online user number is 1
          MAC Addr         Authenticate State           Auth Index
          6805-ca06-557b   MAC_AUTHENTICATOR_SUCCESS     350
…

<Switch> display connection
Slot:  1
Index=350 , Username=68-05-ca-06-55-7b@aabbcc.net
 IP=N/A
 IPv6=N/A
 MAC=6805-ca06-557b

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

Configuration files

```
#
 mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain aabbcc.net
 mac-authentication user-name-format mac-address with-hyphen
#
domain aabbcc.net
 authentication lan-access local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user 68-05-ca-06-55-7b
 password cipher $c$3$KEiYU/nrbJqmp75BldT4m99SzcSQ5Ro3sPRpTvUSd4aGL676
 service-type lan-access
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

Example: Configuring RADIUS-based MAC authentication (MAC-based user account)

Applicable product matrix

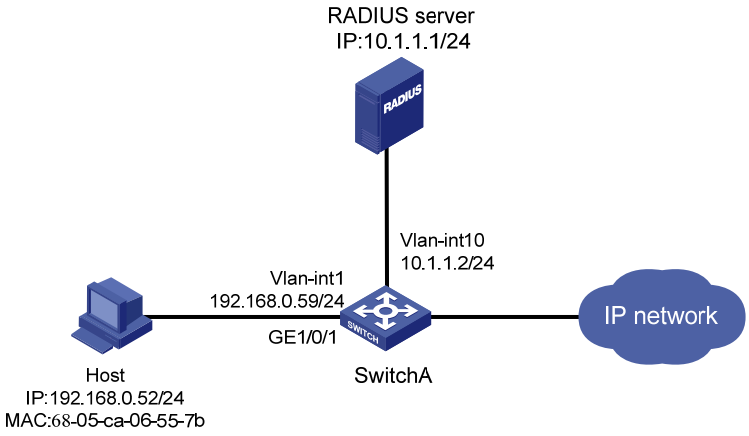
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 113:

- Configure RADIUS-based MAC authentication on the switch to control the network access of users.
- Use the MAC address of each user as the username and password for authentication, and the MAC addresses are hyphenated and in lower case.

Figure 113 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

Configuration restrictions and guidelines

When you configure RADIUS-based MAC authentication, follow these restrictions and guidelines:

- Enable MAC authentication globally only after you have configured the authentication-related parameters. Otherwise, users might fail to pass MAC authentication.

- When you create a user account on the RADIUS server, make sure the account has the same format as the one configured by the **mac-authentication user-name-format** command on the access device.
- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols, but the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. Configure the port used for RADIUS authentication to 1645 for the RADIUS scheme on the access device.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring Switch A

Assign an IP address to each interface as shown in Figure 113. Make sure the host, the switch, and the RADIUS server can reach each other. (Details not shown.)

Configure a RADIUS scheme.

```
<SwitchA> system-view
[SwitchA] radius scheme 2000
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

Create ISP domain **domain2**, and apply the RADIUS scheme to the ISP domain for authentication and authorization of users.

```
[SwitchA] domain domain2
[SwitchA-isp-domain2] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain2] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain2] quit
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
[SwitchA] mac-authentication interface gigabitethernet 1/0/1
 Mac-auth is enabled on port GigabitEthernet 1/0/1.
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain2
```

Set the MAC authentication offline detect timer and quiet timer. The switch detects whether a user has gone offline every 180 seconds. If a user fails MAC authentication, the switch does not authenticate the user within 180 seconds.

```
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180
```

Configure MAC authentication to use MAC-based accounts. The MAC address usernames and passwords are hyphenated and in lower case.

```
[SwitchA] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication globally.

```
[SwitchA] mac-authentication
 Mac-auth is enabled globally.
```

Configuring the RADIUS server

Create RADIUS user **68-05-ca-06-55-7b** (the host's MAC address) on the RADIUS server, and enter RADIUS-server user view.

```
<SwitchB> system-view
[SwitchB] radius-server user 68-05-ca-06-55-7b
[SwitchB-rdsuser-68-05-ca-06-55-7b]
```

Set the password to **123456** in plain text for RADIUS user **68-05-ca-06-55-7b**.

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] password simple 123456
[SwitchB-rdsuser-68-05-ca-06-55-7b] quit
```

Specify RADIUS client **10.1.1.2** and set the shared key to **abc** in plain text.

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

Verifying the configuration

Display MAC authentication settings and statistics.

```
<SwitchA> display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 1
          Current domain is domain2

Silent Mac User info:
         MAC Addr               From Port           Port Index

Gigabitethernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Max number of on-line users is 1
  Current online user number is 1
          MAC Addr         Authenticate State           Auth Index
          6805-ca06-557b   MAC_AUTHENTICATOR_SUCCESS    0
…

<SwitchA> display connection
Slot:  1
Index=0  ,Username=68-05-ca-06-55-7b@domain2
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca06-557b

 Total 1 connection(s) matched on slot 1.
```

```
Total 1 connection(s) matched.
```

Configuration files

- Switch A:

```
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain domain2
 mac-authentication user-name-format mac-address with-hyphen
#
radius scheme 2000
 primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0
+E6g==
 user-name-format without-domain
#
domain domain2
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

- RADIUS server:

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ
==
#
radius-server user 68-05-ca-06-55-7b
 password cipher $c$3$Xv+yKBbrO2yl0iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
#
```

Example: Configuring RADIUS-based MAC authentication (shared user account)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

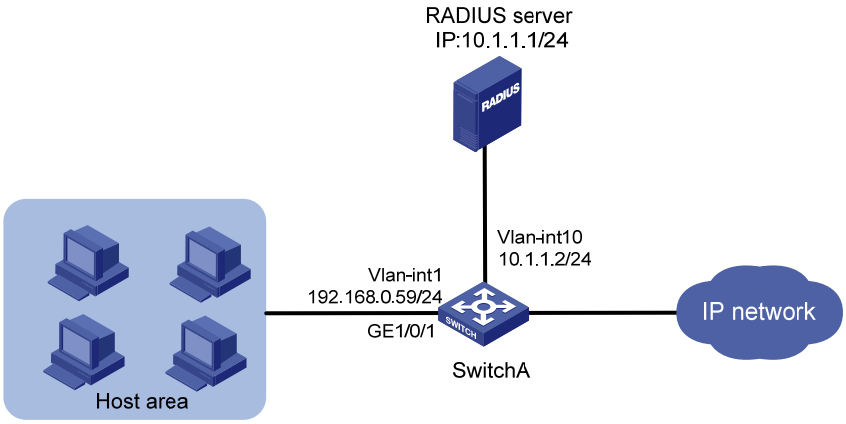
Network requirements

As shown in Figure 114, the hosts are in a secure network.

Configure RADIUS-based MAC authentication on the switch to control the network access of users.

Use a shared user account for all users, with the username **aaa** and password **123456**.

Figure 114 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

Configuration restrictions and guidelines

See "Example: Configuring RADIUS-based MAC authentication (MAC-based user account) ."

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring Switch A

Assign an IP address to each interface as shown in Figure 114. Make sure the hosts, the switch, and the RADIUS server can reach each other. (Details not shown.)

Configure a RADIUS scheme.

```
<SwitchA> system-view
[SwitchA] radius scheme 2000
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

Create ISP domain **domain1**, and apply the RADIUS scheme to the ISP domain for authentication and authorization of users.

```
[SwitchA] domain domain1
[SwitchA-isp-domain1] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain1] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain1] quit
```

#Enable MAC authentication on GigabitEthernet 1/0/1.

```
[SwitchA] mac-authentication interface gigabitethernet 1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain1
```

Set the MAC authentication offline detect timer and quiet timer. The switch detects whether a user has gone offline every 180 seconds. If a user fails authentication, the switch does not authenticate the user within 180 seconds.

```
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180
```

Specify username **aaa** and password **123456** in plain text for the account shared by MAC authentication users.

```
[SwitchA] mac-authentication user-name-format fixed account aaa password simple 123456
```

Enable MAC authentication globally.

```
[SwitchA] mac-authentication
 Mac-auth is enabled globally.
```

Configuring the RADIUS server

Create RADIUS user **aaa** on the RADIUS server, and enter RADIUS-server user view.

```
<SwitchB> system-view
[SwitchB] radius-server user aaa
[SwitchB-rdsuser-aaa]
```

Set the password to **123456** in plain text for RADIUS user **aaa**.

```
[SwitchB-rdsuser-aaa] password simple 123456
[SwitchB-rdsuser-aaa] quit
```

Specify RADIUS client **10.1.1.2** and set the shared key to **abc** in plain text.

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

Verifying the configuration

Display MAC authentication settings and statistics on Switch A.

```
<SwitchA> display mac-authentication
MAC address authentication is enabled.
User name format is fixed account
 Fixed username:aaa
 Fixed password:******
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 4
          Current domain is domain1

Silent Mac User info:
         MAC Addr               From Port           Port Index

Gigabitethernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 4, failed: 0
  Max number of on-line users is 1024
  Current online user number is 4
          MAC Addr         Authenticate State           Auth Index
          6805-ca06-557b   MAC_AUTHENTICATOR_SUCCESS    0
          6805-ca00-8a11   MAC_AUTHENTICATOR_SUCCESS    1
          6805-ca00-6677   MAC_AUTHENTICATOR_SUCCESS    2
          6805-ca02-1122   MAC_AUTHENTICATOR_SUCCESS    3

…

<SwitchA> display connection
Slot:  1
Index=0  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca06-557b
Index=1  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca00-8a11
Index=2  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca00-6677
Index=3  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
```

```
MAC=6805-ca02-1122

Total 4 connection(s) matched on slot 1.
Total 4 connection(s) matched.
```

Configuration files

- Switch A:

```
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain domain1
 mac-authentication user-name-format fixed account aaa password cipher $c$3$6DXU
G/ZZMl7AbkMpJEo2uoni19WCI0nJGw
#
radius scheme 2000
 primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0
+E6g
 user-name-format without-domain
#
domain domain1
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

- RADIUS server:

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ
==
#
radius-server user aaa
 password cipher $c$3$Xv+yKBbrO2yl0iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
#
```

Example: Configuring MAC authentication with ACL assignment

Applicable product matrix

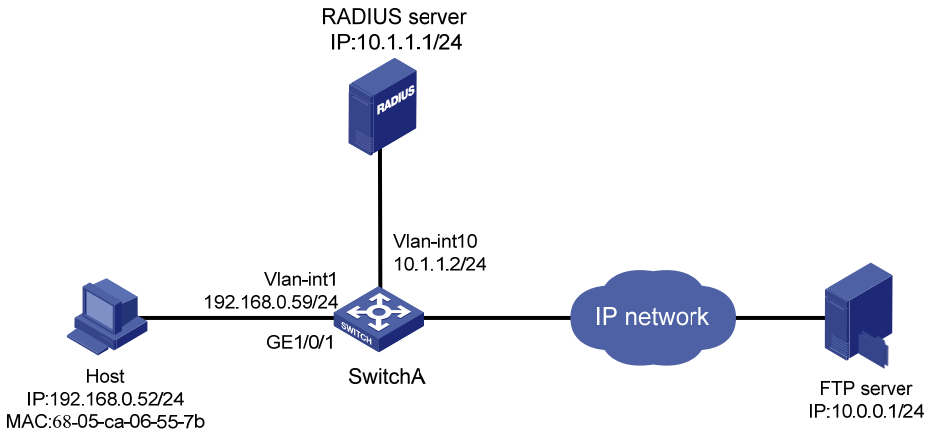
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 115:

- Configure RADIUS-based MAC authentication on the switch to control Internet access of users.
- Apply an ACL to authenticated users to make sure these users can access the Internet but not the FTP server at 10.0.0.1.
- Use MAC-based user accounts for MAC authentication users. The MAC addresses are hyphen-separated and in lower case.

Figure 115 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To meet the network requirements, you must do the following:

- To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.
- To identify valid users, add a user account for each user on the RADIUS server.
- For the switch to implement ACL assignment, configure an ACL on the switch and specify the ACL as the authorization ACL.

Configuration restrictions and guidelines

See "Example: Configuring RADIUS-based MAC authentication (MAC-based user account)."

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring Switch A

Assign an IP address to each interface as shown in Figure 115. Make sure the hosts, the switch, and the RADIUS server can reach each other. (Details not shown.)

Configure a RADIUS scheme.

```
[SwitchA> system-view
[SwitchA] radius scheme 2000
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

Create ISP domain **domain1**, and apply the RADIUS scheme to the ISP domain for authentication and authorization of users.

```
[SwitchA] domain domain1
[SwitchA-isp-domain1] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain1] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain1] quit
```

Configure ACL 3000 to deny packets destined for 10.0.0.1.

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[SwitchA-acl-adv-3000] quit
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
[SwitchA] mac-authentication interface gigabitethernet 1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain1
```

Set the MAC authentication timers.

```
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180
```

Configure the switch to use MAC-based user accounts and the MAC addresses to be hyphen-separated and in lower case.

```
[SwitchA] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication globally.

```
[SwitchA] mac-authentication
 Mac-auth is enabled globally.
```

Configuring the RADIUS server

Add a user account with **68-05-ca-06-55-7b** (the host's MAC address) as the username on the RADIUS server, and enter RADIUS-server user view.

```
<SwitchB> system-view
[SwitchB] radius-server user 68-05-ca-06-55-7b
```

Set the password to **123456** in plain text for the user account.

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] password simple 123456
```

Specify ACL 3000 as the authorization ACL for the user account.

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] authorization-attribute acl 3000
[SwitchB-rdsuser-68-05-ca-06-55-7b] quit
```

Specify RADIUS client **10.1.1.2** and set the shared key to **abc** in plain text.

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

Verifying the configuration

After the host passes authentication, use the **display connection** command on Switch A to display online user information.

```
<SwitchA> display connection
Slot:  1
Index=0  ,Username=68-05-ca-06-55-7b@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca06-557b

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

Ping the FTP server from the host. The output shows that the ACL 3000 has been assigned to port GigabitEthernet 1/0/1 to deny access to the FTP server.

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C:\>
```

Configuration files

- Switch A:

```
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain domain2
```

```
 mac-authentication user-name-format mac-address with-hyphen
#
acl number 3000
 rule 0 deny ip destination 10.0.0.1 0
#
radius scheme 2000
 primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0
+E6g==
 user-name-format without-domain
#
domain domain1
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

- RADIUS server:

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ
==
#
radius-server user 68-05-ca-06-55-7b
 password cipher $c$3$Xv+yKBbrO2yl0iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
 authorization-attribute acl 3000
#
```

MFF configuration examples

This chapter provides MFF configuration examples.

MAC-forced forwarding (MFF) implements Layer 2 isolation and Layer 3 communication between hosts in the same broadcast domain.

Example: Configuring auto-mode MFF in a tree network

Applicable product matrix

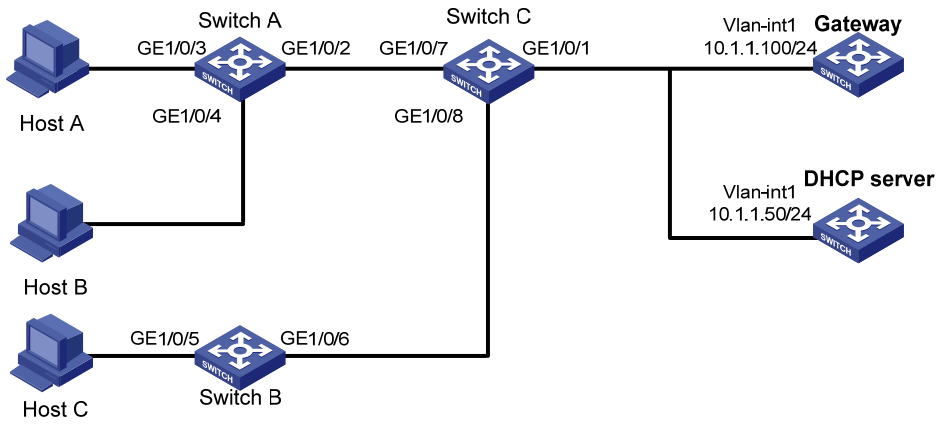
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 116, all devices are in the same VLAN, and the switches form a tree topology. Hosts A, B, and C obtain IP addresses from the DHCP server.

Configure auto-mode MFF on Switch A and Switch B to isolate the hosts at Layer 2 and allow them to communicate with each other through Gateway at Layer 3.

Figure 116 Network diagram



Requirements analysis

To enable the switches to obtain the gateway IP address, you must enable DHCP snooping on Switch A and Switch B.

Configuration procedures

1. On Gateway, configure an IP address for VLAN-interface 1.

```
<Gateway> system-view
[Gateway] interface vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

2. Configure the DHCP server:

   # Enable DHCP and create a DHCP address pool.

```
<Device> system-view
[Device] dhcp enable
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
```

   # Add the gateway's IP address to the DHCP address pool.

```
[Device-dhcp-pool-1] gateway-list 10.1.1.100
[Device-dhcp-pool-1] quit
```

   # Configure an IP address for VLAN-interface 1.

```
[Device] interface vlan-interface 1
[Device-Vlan-interface1] ip address 10.1.1.50 24
```

3. Configure Switch A:

   # Enable DHCP snooping.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

   # Enable MFF in automatic mode.

```
[SwitchA] vlan 1
[SwitchA-vlan1] mac-forced-forwarding auto
[SwitchA-vlan1] quit
```

   # Configure interface GigabitEthernet 1/0/2 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
```

   # Configure GigabitEthernet 1/0/2 as a DHCP snooping trusted port.

```
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
```

4. Configure Switch B:

   # Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

   # Enable MFF in automatic mode.

```
[SwitchB] vlan 1
[SwitchB-vlan1] mac-forced-forwarding auto
[SwitchB-vlan1] quit
```

   # Configure interface GigabitEthernet 1/0/6 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

   # Configure GigabitEthernet 1/0/6 as a DHCP snooping trusted port.

```
[SwitchB-GigabitEthernet1/0/6] dhcp-snooping trust
```

Verifying the configuration

After the configuration is complete, Host A, Host B, and Host C can ping each other. The MAC address in the ARP entry for each host is the Gateway MAC address.

Configuration files

- Gateway:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 10.1.1.100 255.255.255.0
#
```

- DHCP server:

```
#
vlan 1
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
 gateway-list 10.1.1.100
#
interface Vlan-interface1
 ip address 10.1.1.50 255.255.255.0
#
dhcp enable
#
```

- Switch A:

```
#
 dhcp-snooping
#
vlan 1
 mac-forced-forwarding auto
#
interface GigabitEthernet1/0/2
 dhcp-snooping trust
 mac-forced-forwarding network-port
#
```

- Switch B:

```
#
 dhcp-snooping
#
vlan 1
 mac-forced-forwarding auto
#
interface GigabitEthernet1/0/6
 dhcp-snooping trust
```

```
 mac-forced-forwarding network-port
#
```

Example: Configuring auto-mode MFF in a ring network

Applicable product matrix

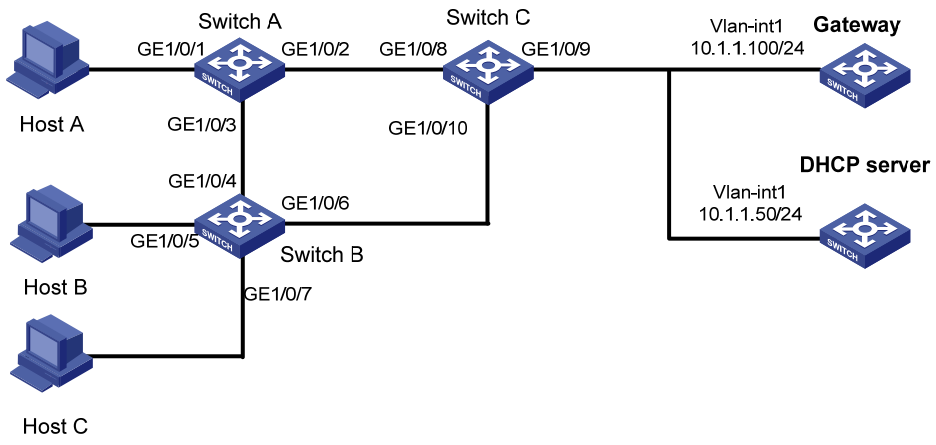
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 117, all devices are in the same VLAN, and the switches form a ring topology. Hosts A, B, and C obtain IP addresses from the DHCP server.

Configure auto-mode MFF on Switch A and Switch B to isolate the hosts at Layer 2 and allow them to communicate with each other through Gateway at Layer 3.

Figure 117 Network diagram



Requirements analysis

To enable the switches to obtain the Gateway IP address, you must enable DHCP snooping on Switch A and Switch B.

To avoid loops, you must enable STP on Switch A, Switch B, and Switch C.

Configuration procedures

1. On Gateway, configure an IP address for VLAN-interface 1.

```
<Gateway> system-view
[Gateway] interface vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

2. Configure the DHCP server:

   # Enable DHCP and create a DHCP address pool.

```
<Device> system-view
[Device] dhcp enable
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
```

   # Add the gateway's IP address to the DHCP address pool.

```
[Device-dhcp-pool-1] gateway-list 10.1.1.100
[Device-dhcp-pool-1] quit
```

   # Configure an IP address for VLAN-interface 1.

```
[Device] interface vlan-interface 1
[Device-Vlan-interface1] ip address 10.1.1.50 24
```

3. Configure Switch A:

   # Enable DHCP snooping.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

   # Enable STP.

```
[SwitchA] stp enable
```

   # Enable MFF in automatic mode.

```
[SwitchA] vlan 1
[SwitchA-vlan1] mac-forced-forwarding auto
[SwitchA-vlan1] quit
```

   # Configure interface GigabitEthernet 1/0/2 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
```

   # Configure GigabitEthernet 1/0/2 as a DHCP snooping trusted port.

```
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/2] quit
```

   # Configure interface GigabitEthernet 1/0/3 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mac-forced-forwarding network-port
```

   # Configure GigabitEthernet 1/0/3 as a DHCP snooping trusted port.

```
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping trust no-user-binding
```

4. Configure Switch B:

   # Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

   # Enable STP.

```
[SwitchB] stp enable
```

Enable MFF in automatic mode.

```
[SwitchB] vlan 1
[SwitchB-vlan1] mac-forced-forwarding auto
[SwitchB-vlan1] quit
```

Configure interface GigabitEthernet 1/0/4 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/4 as a DHCP snooping trusted port.

```
[SwitchB-GigabitEthernet1/0/4] dhcp-snooping trust no-user-binding
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure interface GigabitEthernet 1/0/6 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/6 as a DHCP snooping trusted port.

```
[SwitchB-GigabitEthernet1/0/6] dhcp-snooping trust
```

5. On Switch C, Enable STP.

```
<SwitchC> system-view
[SwitchC] stp enable
```

Verifying the configuration

After the configuration is complete, Host A, Host B, and Host C can ping each other. The MAC address in the ARP entry for each host is the Gateway MAC address.

Configuration files

- Gateway:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 10.1.1.100 255.255.255.0
#
```

- DHCP server:

```
#
vlan 1
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
 gateway-list 10.1.1.100
#
interface Vlan-interface1
 ip address 10.1.1.50 255.255.255.0
#
 dhcp enable
```

```
#
```

- Switch A:

```
#
 dhcp-snooping
#
vlan 1
 mac-forced-forwarding auto
#
 stp enable
#
interface GigabitEthernet1/0/2
 dhcp-snooping trust
 mac-forced-forwarding network-port
#
interface GigabitEthernet1/0/3
 dhcp-snooping trust no-user-binding
 mac-forced-forwarding network-port
#
```

- Switch B:

```
#
 dhcp-snooping
#
vlan 1
 mac-forced-forwarding auto
#
 stp enable
#
interface GigabitEthernet1/0/4
 dhcp-snooping trust no-user-binding
 mac-forced-forwarding network-port
#
interface GigabitEthernet1/0/6
 dhcp-snooping trust
 mac-forced-forwarding network-port
#
```

- Switch C:

```
#
 stp enable
#
```

Example: Configuring manual-mode MFF in a tree network

Applicable product matrix

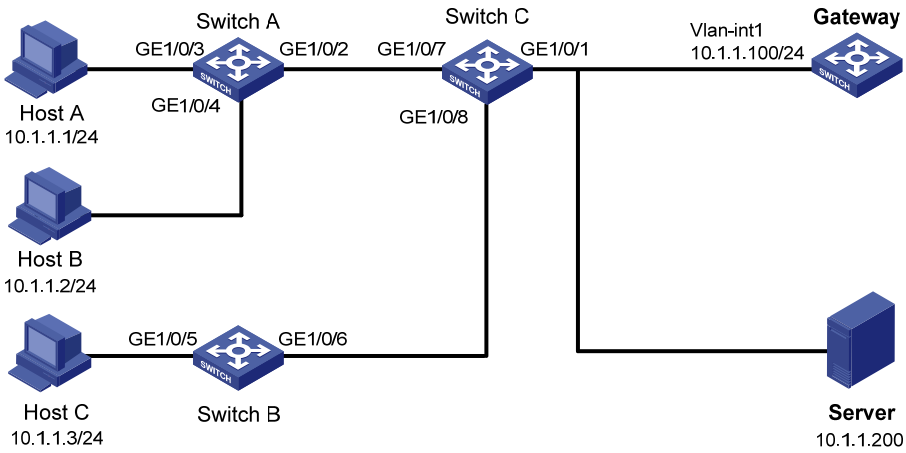
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 118, all devices are in the same VLAN, and the switches form a tree topology. Hosts A, B, and C are assigned IP addresses manually.

Configure manual-mode MFF on Switch A and Switch B to isolate the hosts at Layer 2 and allow them to communicate with each other through Gateway at Layer 3.

Figure 118 Network diagram



Requirements analysis

To allow the MFF-enabled switches to answer ARP requests from the gateway on behalf of hosts, you must enable ARP snooping on the switches.

To ensure the communication between the server and the hosts, you must add the IP address of the server to the server list on Switch A and Switch B.

Configuration procedures

1. Configure IP addresses for the hosts manually as shown in Figure 118.
2. On Gateway, configure an IP address for VLAN-interface 1.

```
<Gateway> system-view
[Gateway] interface vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

3. Configure Switch A:

   # Enable MFF in manual mode.

```
[SwitchA] vlan 1
[SwitchA-vlan1] mac-forced-forwarding default-gateway 10.1.1.100
```

   # Specify the IP address of the server.

```
[SwitchA-vlan1] mac-forced-forwarding server 10.1.1.200
```

   # Enable ARP snooping.

```
[SwitchA-vlan1] arp-snooping enable
[SwitchA-vlan1] quit
```

   # Configure interface GigabitEthernet 1/0/2 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet 1/0/2] mac-forced-forwarding network-port
```

4. Configure Switch B:

   # Enable MFF in manual mode.

```
[SwitchB] vlan 1
[SwitchB-vlan1] mac-forced-forwarding default-gateway 10.1.1.100
```

   # Specify the IP address of the server.

```
[SwitchB-vlan1] mac-forced-forwarding server 10.1.1.200
```

   # Enable ARP snooping.

```
[SwitchB-vlan1] arp-snooping enable
[SwitchB-vlan1] quit
```

   # Configure interface GigabitEthernet 1/0/6 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

Verifying the configuration

After the configuration is complete, Host A, Host B, and Host C can ping each other. The MAC address in the ARP entry for each host is the Gateway MAC address.

Configuration files

- Gateway:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 10.1.1.100 255.255.255.0
#
```

- Switch A:

```
#
vlan 1
```

```
 mac-forced-forwarding default-gateway 10.1.1.100
 mac-forced-forwarding server 10.1.1.200
arp-snooping enable
#
interface GigabitEthernet1/0/2
 mac-forced-forwarding network-port
#
```

- Switch B:

```
#
vlan 1
 mac-forced-forwarding default-gateway 10.1.1.100
 mac-forced-forwarding server 10.1.1.200
arp-snooping enable
#
interface GigabitEthernet1/0/6
 mac-forced-forwarding network-port
#
```

Example: Configuring manual-mode MFF in a ring network

Applicable product matrix

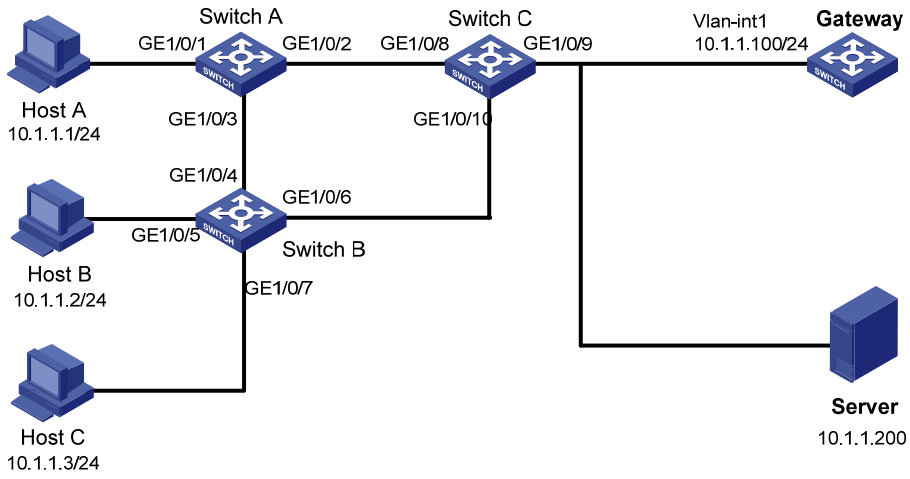
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 119, all the devices are in the same VLAN, and the switches form a ring topology. Hosts A, B, and C are assigned IP addresses manually.

Configure manual-mode MFF on Switch A and Switch B to isolate the hosts at Layer 2 and allow them to communicate with each other through Gateway at Layer 3.

Figure 119 Network diagram



Requirements analysis

For MFF to answer ARP requests from the gateway on behalf of hosts, you must enable ARP snooping.

To ensure the communication between the server and the hosts, you must add the IP address of the server to the server list on Switch A and Switch B.

To avoid loops, you must enable STP on Switch A, Switch B, and Switch C.

Configuration procedures

1. Configure IP addresses for the hosts manually as shown in Figure 119.
2. On Gateway, configure an IP address for VLAN-interface 1.

```
<Gateway> system-view
[Gateway] interface vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

3. Configure Switch A:

   # Enable STP.

```
[SwitchA] stp enable
```

   # Enable MFF in manual mode.

```
[SwitchA] vlan 1
[SwitchA-vlan1] mac-forced-forwarding default-gateway 10.1.1.100
```

   # Specify the IP address of the server.

```
[SwitchA-vlan1] mac-forced-forwarding server 10.1.1.200
```

   # Enable ARP snooping.

```
[SwitchA-vlan1] arp-snooping enable
[SwitchA-vlan1] quit
```

   # Configure interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as network ports.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
[SwitchA-GigabitEthernet1/0/2] quit
```

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mac-forced-forwarding network-port
```

4. Configure Switch B:

   # Enable STP.

   ```
   [SwitchB] stp enable
   ```

   # Enable MFF in manual mode.

   ```
   [SwitchB] vlan 1
   [SwitchB-vlan1] mac-forced-forwarding default-gateway 10.1.1.100
   ```

   # Specify the IP address of the server.

   ```
   [SwitchB-vlan1] mac-forced-forwarding server 10.1.1.200
   ```

   # Enable ARP snooping.

   ```
   [SwitchB-vlan1] arp-snooping enable
   [SwitchB-vlan1] quit
   ```

   # Configure interfaces GigabitEthernet 1/0/4 and GigabitEthernet 1/0/6 as network ports.

   ```
   [SwitchB] interface gigabitethernet 1/0/4
   [SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
   [SwitchB-GigabitEthernet1/0/4] quit
   [SwitchB] interface gigabitethernet 1/0/6
   [SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
   ```

5. On Switch C, enable STP.

   ```
   <SwitchC> system-view
   [SwitchC] stp enable
   ```

Verifying the configuration

After the configuration is complete, Host A, Host B, and Host C can ping each other. The MAC address in the ARP entry for each host is the Gateway MAC address.

Configuration files

- Gateway:

  ```
  #
  vlan 1
  #
  interface Vlan-interface1
   ip address 10.1.1.100 255.255.255.0
  #
  ```

- Switch A:

  ```
  #
  vlan 1
   mac-forced-forwarding default-gateway 10.1.1.100
   mac-forced-forwarding server 10.1.1.200
   arp-snooping enable
  #
   stp enable
  #
  ```

```
interface GigabitEthernet1/0/2
 mac-forced-forwarding network-port
#
interface GigabitEthernet1/0/3
 mac-forced-forwarding network-port
#
```

- Switch B:

```
#
vlan 1
 mac-forced-forwarding default-gateway 10.1.1.100
 mac-forced-forwarding server 10.1.1.200
arp-snooping enable
#
 stp enable
#
interface GigabitEthernet1/0/4
 mac-forced-forwarding network-port
#
interface GigabitEthernet1/0/6
 mac-forced-forwarding network-port
#
```

- Switch C:

```
#
 stp enable
#
```

Mirroring configuration examples

This chapter provides mirroring configuration examples.

Table 12 Mirroring types and scenarios

Mirroring type	Application scenario
Port mirroring	All traffic to be monitored is forwarded to the switch that connects to the data monitoring device.
Layer 2 remote mirroring	The mirroring source and mirroring destination are located on different devices on the same Layer 2 network.
Layer 3 remote mirroring	The mirroring source and the mirroring destination are separated by IP networks.
Local traffic mirroring	The device that monitors the traffic is directly connected to the device that the traffic passes through.
Remote traffic mirroring	The device that monitors the traffic is *not* directly connected to the device that the traffic passes through.

Example: Configuring local port mirroring

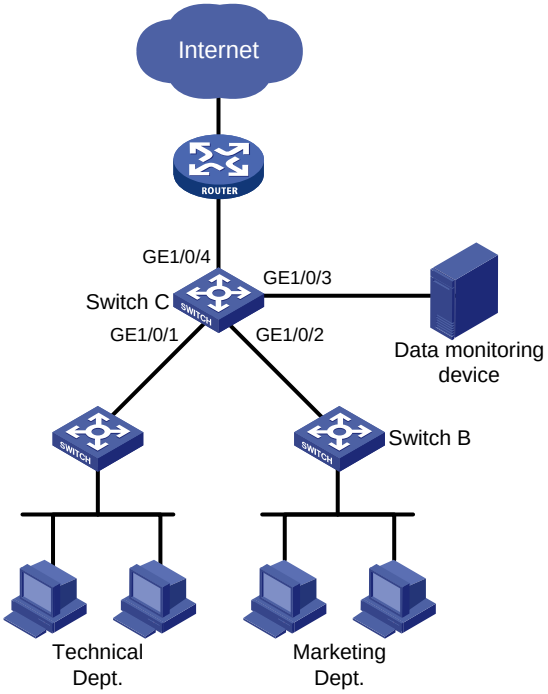
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 120, configure local port mirroring to monitor the Internet traffic and bidirectional traffic of the Marketing Department and the Technical Department.

Figure 120 Network diagram



Configuration restrictions and guidelines

When you configure local port mirroring, follow these restrictions and guidelines:

- A local mirroring group takes effect only when both source ports and the monitor port are configured. Do not configure a port of an existing mirroring group as the source port or the monitor port.
- Use a monitor port only for port mirroring. This is to make sure the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and correctly forwarded traffic.

Configuration procedures

Create local mirroring group 1.

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 local
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as the source ports of the mirroring group, and configure the mirroring group to monitor the incoming traffic of the ports.

```
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
inbound
```

Configure GigabitEthernet 1/0/3 as the monitor port of the mirroring group.

```
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

Disable the spanning tree feature on GigabitEthernet 1/0/3 to make sure mirroring operates correctly.

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo stp enable
[SwitchC-GigabitEthernet1/0/3] quit
```

Verifying the configuration

After the configurations are complete, display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
        GigabitEthernet1/0/2  inbound
    monitor port: GigabitEthernet1/0/3
```

Configuration files

```
#
 mirroring-group 1 local
#
interface GigabitEthernet1/0/1
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
 stp disable
 mirroring-group 1 monitor-port
#
```

Example: Configuring Layer 2 remote port mirroring

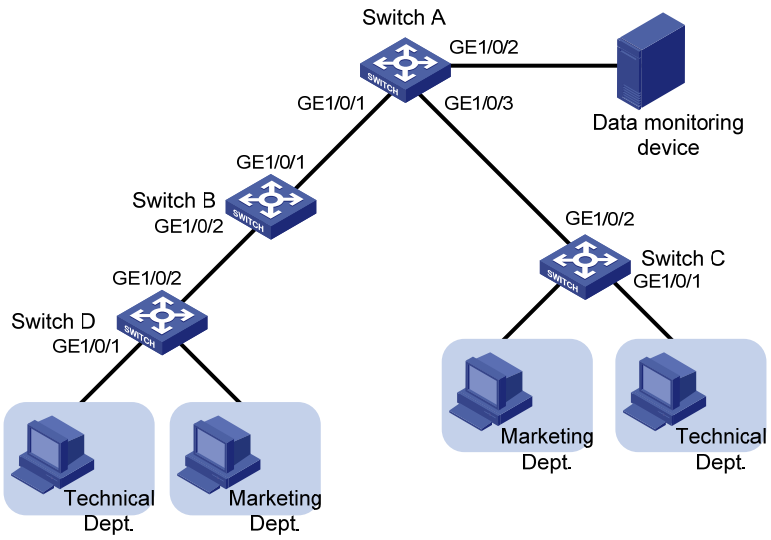
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 121, configure Layer 2 remote port mirroring to monitor the outgoing traffic of the Technical Departments.

Figure 121 Network diagram



Configuration restrictions and guidelines

When you configure the source device, follow these restrictions and guidelines:

- A remote source group contains only one egress port.
- You cannot configure a port of an existing mirroring group as an egress port.
- Only a static VLAN that already exists can be configured as a remote probe VLAN.
- Use a remote probe VLAN only for port mirroring.
- A remote probe VLAN belongs to only one remote source group.
- Specify an unused VLAN as the remote probe VLAN.

When you configure the destination device, follow these restrictions and guidelines:

- You cannot configure a port of an existing mirroring group as a destination port.
- Use a monitor port only for port mirroring.
- Only a static VLAN that already exists can be configured as a remote probe VLAN.
- Use a remote probe VLAN only for port mirroring.
- A remote probe VLAN belongs to only one remote destination group.
- Specify an unused VLAN as the remote probe VLAN.

Configuration procedures

Configuring Switch A (the destination device)

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 as trunk ports to permit the packets from VLAN 2 to pass through.

```
<SwitchA> system-view
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/3] quit
```

Create a remote destination group.

```
[SwitchA] mirroring-group 1 remote-destination
```

Create VLAN 2, which is to be configured as the remote probe VLAN.

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

Configure VLAN 2 as the remote probe VLAN and GigabitEthernet 1/0/2 as the monitor port in the mirroring group.

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
[SwitchA] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

Assign the monitor port to VLAN 2. The mirrored packets do not need to be VLAN tagged, so configure the monitor port as an access port.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port access vlan 2
```

Disable the spanning tree feature on GigabitEthernet 1/0/2 to make sure mirroring operates correctly.

```
[SwitchC-GigabitEthernet1/0/2] undo stp enable
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B (the intermediate device)

Create VLAN 2, which is to be configured as the remote probe VLAN.

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

Configure GigabitEthernet 1/0/1 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/2] quit
```

Configuring Switch C and Switch D (the source device)

Create a remote source group.

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 remote-source
```

Create VLAN 2, which is to be configured as the remote probe VLAN.

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

Configure VLAN 2 as the remote probe VLAN.

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
```

Configure the mirroring group to monitor the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 inbound
```

Configure GigabitEthernet 1/0/2 as the egress port.

```
[SwitchC] mirroring-group 1 monitor-egress GigabitEthernet 1/0/2
```

Configure GigabitEthernet 1/0/2 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 2
[SwitchC-GigabitEthernet1/0/2] quit
```

Disable the spanning tree and MAC address learning features on GigabitEthernet 1/0/2 to make sure mirroring operates correctly.

```
[SwitchC-GigabitEthernet1/0/2] undo stp enable
[SwitchC-GigabitEthernet1/0/2] mac-address mac-learning disable
[SwitchC-GigabitEthernet1/0/2] quit
```

NOTE:

Configure Switch D in the same way that Switch C is configured. Details are not shown here.

Verifying the configuration

After the configurations are complete, display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
mirroring-group 1:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
    reflector port:
    monitor egress port: GigabitEthernet1/0/2
    remote-probe VLAN: 2
```

Display information about mirroring group 1 on Switch A.

```
[SwitchA]display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/0/2
    remote-probe VLAN: 2
```

Configuration files

- Switch A:

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port access vlan 2
 stp disable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 to 2
```

- Switch B:

```
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 2
#
```

- Switch C:

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface GigabitEthernet1/0/1
 mirroring-group 1 mirroring-port
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 2
 stp disable
```

```
 mac-address mac-learning disable
 mirroring-group 1 monitor-egress
#
```

Example: Configuring Layer 3 remote port mirroring

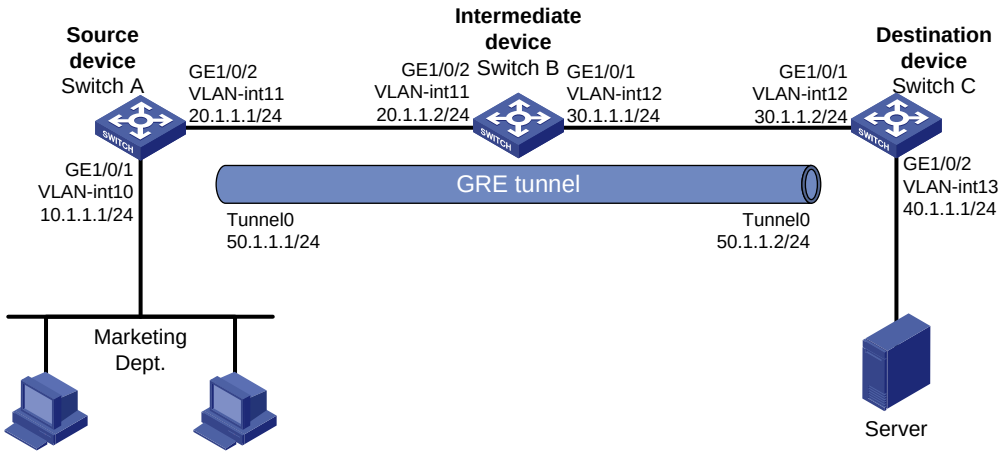
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 122, the network uses OSPF to advertise routes between the subnets. Configure Layer 3 remote port mirroring to monitor the bidirectional traffic of the Marketing Department.

Figure 122 Network diagram



Configuration restrictions and guidelines

When you configure a GRE over IPv4 tunnel to connect the company, the tunnel source and destination identify the tunnel. Make sure of the following:

- The configurations on the tunnel ends are the same.
- The source/destination address for an end is the destination/source for the remote end.

Configuration procedures

Configuring Switch A (the source device)

Create VLAN-interface 10 and VLAN-interface 11.

```
<SwitchA> system-view
[SwitchA] vlan 10 to 11
 Please wait... Done.
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.1.1.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] interface Vlan-interface 11
[SwitchA-Vlan-interface11] ip address 20.1.1.1 24
[SwitchA-Vlan-interface11] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 10 and GigabitEthernet 1/0/2 to VLAN 11.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port access vlan 10
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 11
[SwitchA-GigabitEthernet1/0/2] quit
```

Create tunnel interface Tunnel 0, and configure its IP address and mask.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ip address 50.1.1.1 24
```

Configure Tunnel 0 to operate in GRE over IPv4 tunnel mode, and configure the source and destination IP addresses for it.

```
[SwitchA-Tunnel0] tunnel-protocol gre
[SwitchA-Tunnel0] source 20.1.1.1
[SwitchA-Tunnel0] destination 30.1.1.2
[SwitchA-Tunnel0] quit
```

Configure service loopback group 1 and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign an unused port (GigabitEthernet 1/0/3, in this example) to service loopback group 1.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Reference service loopback group 1 on the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Enable the OSPF protocol to advertise routes to the subnets where the VLAN interfaces and the tunnel interface reside.

```
[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 20.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Create local mirroring group 1.

```
[SwitchA] mirroring-group 1 local
```

Configure GigabitEthernet 1/0/1 as a source port and Tunnel 0 as the monitor port of local mirroring group 1.

```
[SwitchA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
[SwitchA] mirroring-group 1 monitor-port tunnel 0
```

Configuring Switch B (the intermediate device)

Create VLAN-interface 11 and VLAN-interface 12.

```
<SwitchB> system-view
[SwitchB] vlan 11 to 12
 Please wait... Done.
[SwitchB] interface Vlan-interface 11
[SwitchB-Vlan-interface11] ip address 20.1.1.2 24
[SwitchB-Vlan-interface11] quit
[SwitchB] interface Vlan-interface 12
[SwitchB-Vlan-interface12] ip address 30.1.1.1 24
[SwitchB-Vlan-interface12] quit
```

Assign GigabitEthernet 1/0/2 to VLAN 11 and GigabitEthernet 1/0/1 to VLAN 12.

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 11
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 12
[SwitchB-GigabitEthernet1/0/1] quit
```

Enable the OSPF protocol to advertise routes to the subnets where VLAN-interface 11 and VLAN-interface 12 reside.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configuring Switch C (the destination device)

Create VLAN-interface 12 and VLAN-interface 13.

```
<SwitchC> system-view
[SwitchC] vlan 12 to 13
 Please wait... Done.
[SwitchC] interface Vlan-interface 12
```

```
[SwitchC-Vlan-interface12] ip address 30.1.1.2 24
[SwitchC-Vlan-interface12] quit
[SwitchC] interface Vlan-interface 13
[SwitchC-Vlan-interface13] ip address 40.1.1.1 24
```

Assign GigabitEthernet 1/0/1 to VLAN 12 and GigabitEthernet 1/0/2 to VLAN 13.

```
[SwitchC-Vlan-interface13] quit
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 12
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 13
[SwitchC-GigabitEthernet1/0/2] quit
```

Create tunnel interface Tunnel 0, and configure its IP address and mask.

```
[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] ip address 50.1.1.2 24
```

Configure Tunnel 0 to operate in GRE over IPv4 tunnel mode, and configure the source and destination IP addresses for it.

```
[SwitchC-Tunnel0] tunnel-protocol gre
[SwitchC-Tunnel0] source 30.1.1.2
[SwitchC-Tunnel0] destination 20.1.1.1
[SwitchC-Tunnel0] quit
```

Configure service loopback group 1 and specify its service type as **tunnel**.

```
[SwitchC] service-loopback group 1 type tunnel
```

Assign an unused port (GigabitEthernet 1/0/3, in this example) to service loopback group 1.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo stp enable
[SwitchC-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchC-GigabitEthernet1/0/3] quit
```

Reference service loopback group 1 on the tunnel interface.

```
[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] service-loopback-group 1
[SwitchC-Tunnel0] quit
```

Enable the OSPF protocol to advertise routes to the subnets where the VLAN interfaces and the tunnel interface reside.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Create local mirroring group 1.

```
[SwitchA] mirroring-group 1 local
```

Configure the mirroring group to monitor the incoming traffic of the source port GigabitEthernet 1/0/1.

```
[SwitchC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
```

Configure GigabitEthernet 1/0/2 as the monitor port of local mirroring group 1.

```
[SwitchC] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

Verifying the configuration

After the configurations are complete, display information about mirroring group 1 on Switch A.

```
[SwitchA] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  both
    monitor port: Tunnel0
```

Display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
    monitor port: GigabitEthernet1/0/2
```

Configuration files

- Switch A:

```
#
 mirroring-group 1 local
#
 service-loopback group 1 type tunnel
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface11
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 10
 mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/0/2
 port link-type trunk
```

```
 port trunk permit vlan 1 11
#
interface GigabitEthernet1/0/3
 stp disable
 port service-loopback group 1
#
interface Tunnel0
 ip address 50.1.1.1 255.255.255.0
 source 20.1.1.1
 destination 30.1.1.2
 service-loopback-group 1
 mirroring-group 1 monitor-port
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 50.1.1.0 0.0.0.255
```

- Switch B:

```
#
vlan 11 to 12
#
interface Vlan-interface11
 ip address 20.1.1.2 255.255.255.0
#
interface Vlan-interface12
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
 port trunk permit vlan 1 12
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 11
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
```

- Switch C:

```
#
 mirroring-group 1 local
#
 service-loopback group 1 type tunnel
#
vlan 12 to 13
#
```

```
interface Vlan-interface12
 ip address 30.1.1.2 255.255.255.0
#
interface Vlan-interface13
 ip address 40.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 12
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port access vlan 13
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/3
 stp disable
 port service-loopback group 1
#
interface Tunnel0
 ip address 50.1.1.1 255.255.255.0
 source 30.1.1.2
 destination 20.1.1.1
 service-loopback-group 1
#
ospf 1
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  network 50.1.1.0 0.0.0.255
```

Example: Configuring local traffic mirroring

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

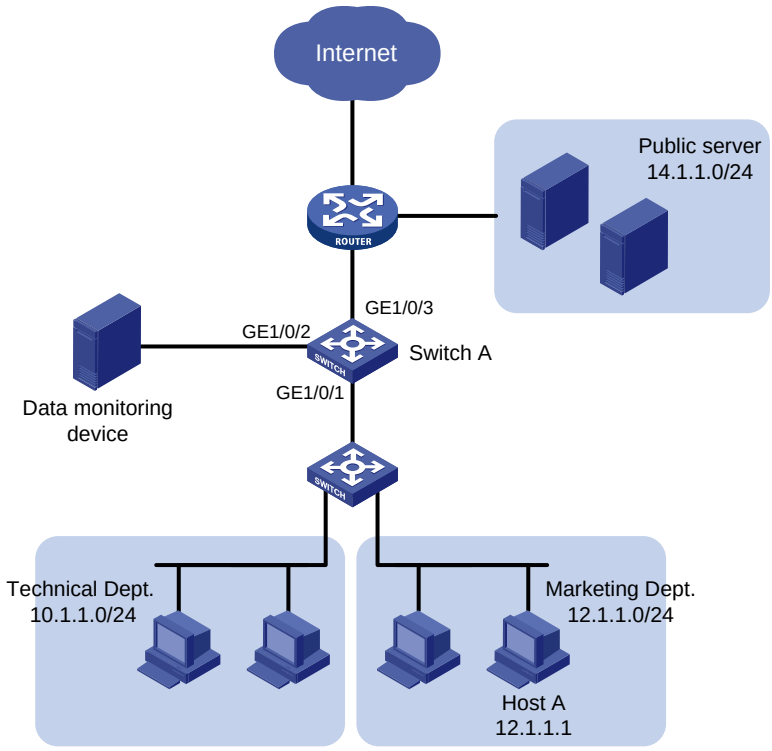
Network requirements

As shown in Figure 123, configure local traffic mirroring to mirror the following traffic:

- HTTP traffic sent by the Technical Department to access the Internet.

- Packets that Host A in the Marketing Department receives from the public server cluster during non-working hours from 18:00 to 08:30 (the next day) on working days.

Figure 123 Network diagram



Configuration procedures

1. Configure a QoS policy that mirrors Internet traffic from the Technical Department:

   # Create ACL 3000 and configure a rule to permit packets from the Technical Department to access the Internet.

   ```
   <SwitchA> system-view
   [SwitchA] acl number 3000
   [SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 10.1.1.0
   0.0.0.255
   [SwitchA-acl-adv-3000] quit
   ```

   # Create traffic class **classifier_research**, and then configure the match criterion as ACL 3000.

   ```
   [SwitchA] traffic classifier classifier_research
   [SwitchA-classifier-classifier_research] if-match acl 3000
   [SwitchA-classifier-classifier_research] quit
   ```

   # Create traffic behavior **behavior_research**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/2.

   ```
   [SwitchA] traffic behavior behavior_research
   [SwitchA-behavior-behavior_research] mirror-to interface GigabitEthernet 1/0/2
   [SwitchA-behavior-behavior_research] quit
   ```

   # Create QoS policy **policy_research**, and then associate traffic class **classifier_research** with traffic behavior **behavior_research** in the QoS policy.

   ```
   [SwitchA] qos policy policy_research
   ```

```
[SwitchA-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
[SwitchA-qospolicy-policy_research] quit
```

2. Configure a QoS policy that mirrors traffic received by Host A from the public server:

   # Configure two time ranges named **off-work1** and **off-work2** to cover the time from 0:00 to 8:30 and 18:00 to 24:00 on working days, respectively.

```
[SwitchA] time-range off-work1 0:00 to 8:30 working-day
[SwitchA] time-range off-work2 18:00 to 24:00 working-day
```

   # Create ACL 3001, and configure two rules to permit packets from the public server to Host A in non-working hours on working days.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work1
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work2
[SwitchA-acl-adv-3001] quit
```

   # Create traffic class **classifier_market**, and then configure the match criterion as ACL 3001.

```
[SwitchA] traffic classifier classifier_market
[SwitchA-classifier-classifier_market] if-match acl 3001
[SwitchA-classifier-classifier_market] quit
```

   # Create traffic behavior **behavior_market**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/2.

```
[SwitchA] traffic behavior behavior_market
[SwitchA-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/2
[SwitchA-behavior-behavior_market] quit
```

   # Create QoS policy **policy_market**, and then associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[SwitchA] qos policy policy_market
[SwitchA-qospolicy-policy_market] classifier classifier_market behavior
behavior_market
[SwitchA-qospolicy-policy_market] quit
```

3. Apply the QoS policies:

   # Apply QoS policy **policy_research** to the incoming packets of GigabitEthernet 1/0/1.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy policy_research inbound
```

   # Apply QoS policy **policy_market** to the outgoing packets of GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] qos apply policy policy_market outbound
[SwitchA-GigabitEthernet1/0/1] quit
```

Verifying the configuration

After the configurations are complete, display local traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface GigabitEthernet 1/0/1

  Interface: GigabitEthernet1/0/1

  Direction: Inbound
```

```
  Policy: policy_research
   Classifier: classifier_research
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: behavior_research
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet1/0/2

  Direction: Outbound

  Policy: policy_market
   Classifier: classifier_market
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: behavior_market
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet1/0/2
```

Configuration files

```
#
 time-range off-work1 00:00 to 08:30 working-day
 time-range off-work2 18:00 to 24:00 working-day
#
acl number 3000
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range off-work1
 rule 5 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range off-work2
#
traffic classifier classifier_research operator and
 if-match acl 3000
traffic classifier classifier_market operator and
 if-match acl 3001
#
traffic behavior behavior_research
 mirror-to interface GigabitEthernet1/0/2
traffic behavior behavior_market
 mirror-to interface GigabitEthernet1/0/2
#
qos policy policy_research
 classifier classifier_research behavior behavior_research
qos policy policy_market
 classifier classifier_market behavior behavior_market
#
```

```
interface GigabitEthernet1/0/1
 qos apply policy policy_research inbound
 qos apply policy policy_market outbound
```

Example: Configuring remote traffic mirroring

Applicable product matrix

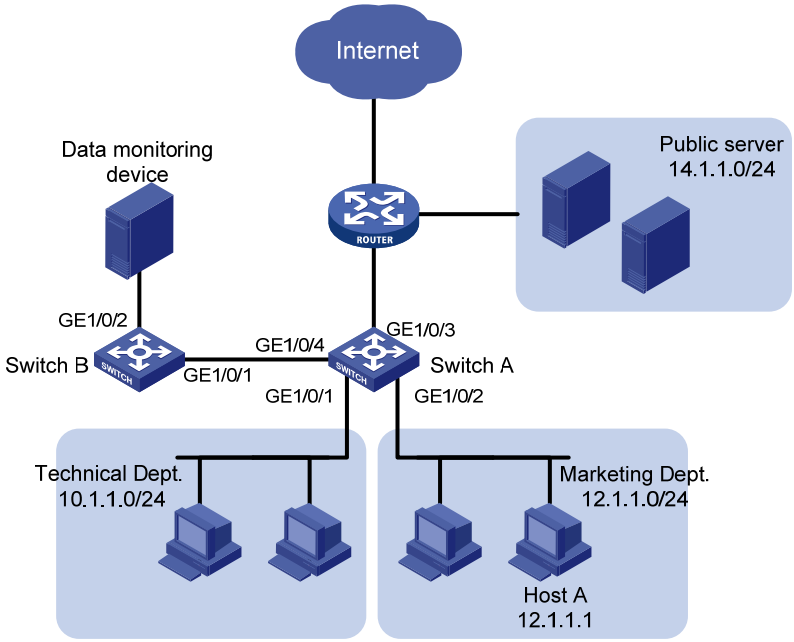
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 124, configure remote traffic mirroring to mirror the following traffic:

- HTTP traffic sent by the Technical Department to access the Internet.
- Packets that Host A in the Marketing Department receives from the public server cluster during the non-working hours from 18:00 to 8:30 (the next day) on working days.

Figure 124 Network diagram



Configuration restrictions and guidelines

Remote traffic mirroring is implemented by local traffic mirroring and Layer 2 remote port mirroring. For the related configuration restrictions and guidelines, see "Configuration restrictions and guidelines."

Configuration procedures

Configuring Switch A

Create ACL 3000, and configure a rule to permit packets from the Technical Department to access the Internet.

```
<SwitchA> system-view
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 10.1.1.0 0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Create traffic class **classifier_research**, and then configure the match criterion as ACL 3000.

```
[SwitchA] traffic classifier classifier_research
[SwitchA-classifier-classifier_research] if-match acl 3000
[SwitchA-classifier-classifier_research] quit
```

Create traffic behavior **behavior_research**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/4.

```
[SwitchA] traffic behavior behavior_research
[SwitchA-behavior-behavior_research] mirror-to interface GigabitEthernet 1/0/4
[SwitchA-behavior-behavior_research] quit
```

Create QoS policy **policy_research**, and then associate traffic class **classifier_research** with traffic behavior **behavior_research** in the QoS policy.

```
[SwitchA] qos policy policy_research
[SwitchA-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
[SwitchA-qospolicy-policy_research] quit
```

Configure two time ranges named **off-work1** and **off-work2** to cover the time from 0:00 to 8:30 and 18:00 to 24:00 on working days, respectively.

```
[SwitchA] time-range off-work1 0:00 to 8:30 working-day
[SwitchA] time-range off-work2 18:00 to 24:00 working-day
```

Create ACL 3001, and configure two rules to permit packets from the public server to Host A in non-working hours on working days.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work1
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work2
[SwitchA-acl-adv-3001] quit
```

Create traffic class **classifier_market**, and then configure the match criterion as ACL 3001.

```
[SwitchA] traffic classifier classifier_market
[SwitchA-classifier-classifier_market] if-match acl 3001
[SwitchA-classifier-classifier_market] quit
```

Create traffic behavior **behavior_market**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/4.

```
[SwitchA] traffic behavior behavior_market
[SwitchA-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/4
[SwitchA-behavior-behavior_market] quit
```

Create QoS policy **policy_market**, and then associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[SwitchA] qos policy policy_market
[SwitchA-qospolicy-policy_market] classifier classifier_market behavior behavior_market
[SwitchA-qospolicy-policy_market] quit
```

Apply QoS policy **policy_research** to the incoming packets of GigabitEthernet 1/0/1.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy policy_research inbound
[SwitchA-GigabitEthernet1/0/1] quit
```

Apply QoS policy **policy_market** to the outgoing packets of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy policy_market outbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Create remote source group 1.

```
[SwitchA] mirroring-group 1 remote-source
```

Configure an unused VLAN (VLAN 2, in this example) as the remote probe VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] mirroring-group 1 remote-probe vlan 2
```

Configure an unused port (GigabitEthernet 1/0/10, in this example) as a source port and GigabitEthernet 1/0/4 as the egress port of remote source group 1.

```
[SwitchA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/10 inbound
[SwitchA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/4
```

NOTE:

Configure an unused port as a source port to prevent packets that pass through the port from being mirrored to the destination device through the remote mirroring group.

Configure GigabitEthernet 1/0/4 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/4] quit
```

Configuring Switch B

Configure GigabitEthernet 1/0/1 as a trunk port to permit the packets from VLAN 2 to pass through.

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

Create remote destination group 1.

```
[SwitchB] mirroring-group 1 remote-destination
```

Configure VLAN 2 as the remote probe VLAN.

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

```
[SwitchB] mirroring-group 1 remote-probe vlan 2
```

Configure GigabitEthernet 1/0/2 as the monitor port of the remote destination group.

```
[SwitchB] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

Assign the monitor port to VLAN 2. The mirrored packets do not need to be VLAN tagged, so configure the monitor port as an access port.

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port access vlan 2
[SwitchB-GigabitEthernet1/0/2] quit
```

Verifying the configuration

After the configurations are complete, display remote traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface

  Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: policy_research
   Classifier: classifier_research
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: behavior_research
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet1/0/4

  Interface: GigabitEthernet1/0/2

  Direction: Outbound

  Policy: policy_market
   Classifier: classifier_market
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: behavior_market
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet1/0/4
```

Display information about mirroring group 1 on Switch A.

```
 [SwitchA] display mirroring-group 1
mirroring-group 1:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet1/0/10  inbound
    reflector port:
```

```
    monitor egress port: GigabitEthernet1/0/4
    remote-probe VLAN: 2
```

Display information about mirroring group 1 on Switch B.

```
[SwitchB] display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/0/2
    remote-probe VLAN: 2
```

Configuration files

- Switch A:

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 2
#
 time-range off-work1 00:00 to 08:30 working-day
 time-range off-work2 18:00 to 24:00 working-day
#
acl number 3000
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range
off-work1
 rule 5 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range
off-work2
#
vlan 2
#
traffic classifier classifier_research operator and
 if-match acl 3000
traffic classifier classifier_market operator and
 if-match acl 3001
#
traffic behavior behavior_research
 mirror-to interface GigabitEthernet1/0/4
traffic behavior behavior_market
 mirror-to interface GigabitEthernet1/0/4
#
qos policy policy_market
 classifier classifier_market behavior behavior_market
qos policy policy_research
 classifier classifier_research behavior behavior_research
#
interface GigabitEthernet1/0/1
 qos apply policy policy_research inbound
#
```

```
interface GigabitEthernet1/0/2
 qos apply policy policy_market outbound
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 to 2
 mirroring-group 1 monitor-egress
#
interface GigabitEthernet1/0/10
 mirroring-group 1 mirroring-port inbound
```

- Switch B:

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 2
#
vlan 2
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port access vlan 2
 mirroring-group 1 monitor-port
```

Example: Configuring traffic mirroring in a flexible way

Applicable product matrix

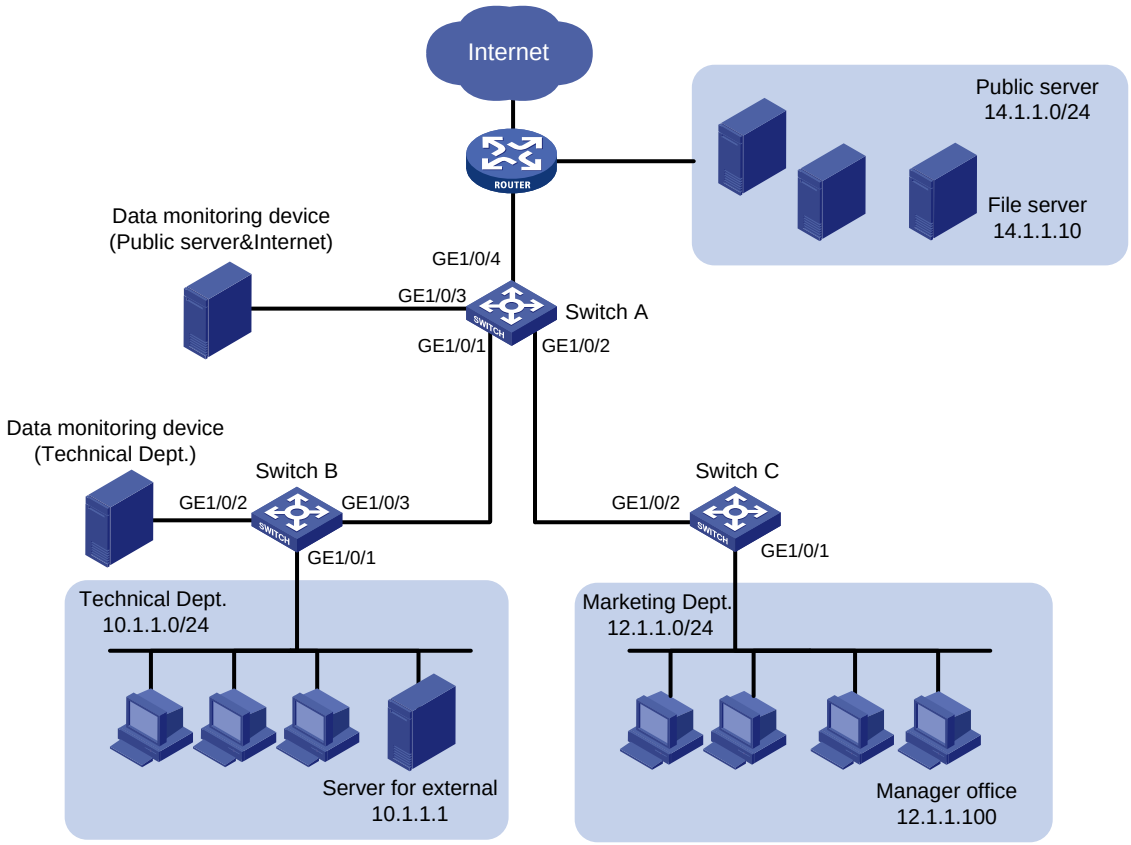
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 125, configure traffic mirroring to monitor the network traffic by using the data monitoring devices as follows:

- Monitor the traffic from public servers. Monitor the traffic from the file server only in the non-working hours (18:00 to 8:30 of the next day) on working days.
- Monitor the traffic from the Marketing Department to the Internet, but do not monitor the traffic from the Marketing Department manager office to the Internet.
- Monitor the traffic from the Technical Department only in non-working hours (18:00 to 8:30 of the next day) on working days.

Figure 125 Network diagram



Requirements analysis

To filter data from a specific source, use one of the following methods:

- Apply a QoS policy of denying traffic to the outgoing interface of the mirrored data. The data from the specified source is not received by the data monitoring device.
- Configure a class-behavior association to permit the data from the specified source, and then issue the class-behavior association before the class-behavior association for mirroring. Data from the specified source is not mirrored.
- Use the **packet-filter** command on the outgoing interface of the mirrored data. The data from the specified source is not received by the data monitoring device.

Configuration procedures

Configuring Switch A to mirror traffic from the public servers

1. Configure a QoS policy to mirror traffic from all public servers:

   # Create ACL 2000 to permit packets from subnet 14.1.1.0/24.

```
<SwitchA> system-view
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 14.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

Create traffic class **classifier_servers**, and then configure the match criterion as ACL 2000.

```
[SwitchA] traffic classifier classifier_servers
[SwitchA-classifier-classifier_servers] if-match acl 2000
[SwitchA-classifier-classifier_servers] quit
```

Create traffic behavior **behavior_servers**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/3.

```
[SwitchA] traffic behavior behavior_servers
[SwitchA-behavior-behavior_servers] mirror-to interface GigabitEthernet 1/0/3
[SwitchA-behavior-behavior_servers] quit
```

Create QoS policy **policy_servers**, and then associate traffic class **classifier_servers** with traffic behavior **behavior_servers** in the QoS policy.

```
[SwitchA] qos policy policy_servers
[SwitchA-qospolicy-policy_servers] classifier classifier_servers behavior
behavior_servers
[SwitchA-qospolicy-policy_servers] quit
```

Apply QoS policy **policy_servers** to the incoming packets of GigabitEthernet 1/0/4.

```
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] qos apply policy policy_servers inbound
[SwitchA-GigabitEthernet1/0/4] quit
```

2. Configure a QoS policy to filter packets from the file server in working hours:

Create a working hour range named **work-time**, in which the working hour is from 8:30 to 18:00 on working days.

```
[SwitchA] time-range work-time 8:30 to 18:00 working-day
```

Create ACL 2001, and configure a rule to permit packets from 14.1.1.10 in working hours on working days.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 14.1.1.10 0.0.0.0 time-range work-time
[SwitchA-acl-basic-2001] quit
```

Create traffic class **classifier_fileserver**, and then configure the match criterion as ACL 2001.

```
[SwitchA] traffic classifier classifier_fileserver
[SwitchA-classifier-classifier_fileserver] if-match acl 2001
[SwitchA-classifier-classifier_fileserver] quit
```

Create traffic behavior **behavior_fileserver**, and then configure the action of denying traffic.

```
[SwitchA] traffic behavior behavior_fileserver
[SwitchA-behavior-behavior_fileserver] filter deny
[SwitchA-behavior-behavior_fileserver] quit
```

Create QoS policy **policy_fileserver**, and then associate traffic class **classifier_fileserver** with traffic behavior **behavior_fileserver** in the QoS policy.

```
[SwitchA] qos policy policy_fileserver
[SwitchA-qospolicy-policy_fileserver] classifier classifier_fileserver behavior
behavior_fileserver
[SwitchA-qospolicy-policy_fileserver] quit
```

Apply QoS policy **policy_fileserver** to the outgoing packets of GigabitEthernet 1/0/3.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] qos apply policy policy_servers outbound
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch A to mirror traffic from the Marketing Department to access the Internet

1. Create a traffic class and a traffic behavior for the packets:

   # Create ACL 3000, and configure a rule to permit packets from subnet 12.1.1.0/24.

   ```
   [SwitchA] acl number 3000
   [SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 12.1.1.0
   0.0.0.255
   [SwitchA-acl-adv-3000] quit
   ```

   # Create traffic class **classifier_market**, and then configure the match criterion as ACL 3000.

   ```
   [SwitchA] traffic classifier classifier_market
   [SwitchA-classifier-classifier_market] if-match acl 3000
   [SwitchA-classifier-classifier_market] quit
   ```

   # Create traffic behavior **behavior_market**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/3.

   ```
   [SwitchA] traffic behavior behavior_market
   [SwitchA-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/3
   [SwitchA-behavior-behavior_market] quit
   ```

2. Create a traffic class and a traffic behavior for the packets from the manager office:

   # Create ACL 3001, and configure a rule to permit packets from 12.1.1.100.

   ```
   [SwitchA] acl number 3001
   [SwitchA-acl-adv-3001] rule permit tcp destination-port eq 80 source 12.1.1.100
   0.0.0.0
   [SwitchA-acl-adv-3001] quit
   ```

   # Create traffic class **classifier_market_mgr**, and then configure the match criterion as ACL 3001.

   ```
   [SwitchA] traffic classifier classifier_market_mgr
   [SwitchA-classifier-classifier_market_mgr] if-match acl 3001
   [SwitchA-classifier-classifier_market_mgr] quit
   ```

   # Create traffic behavior **behavior_market_mgr**, and then configure the action of permitting traffic to pass through.

   ```
   [SwitchA] traffic behavior behavior_market_mgr
   [SwitchA-behavior-behavior_market_mgr] filter permit
   [SwitchA-behavior-behavior_market_mgr] quit
   ```

3. Create a QoS policy to associate the traffic classes and traffic behaviors:

   # Create QoS policy **policy_market**.

   ```
   [SwitchA] qos policy policy_market
   ```

   # Associate traffic class **classifier_market_mgr** with traffic behavior **behavior_market_mgr** in the QoS policy.

   ```
   [SwitchA-qospolicy-policy_market] classifier classifier_market_mgr behavior
   behavior_market_mgr
   ```

   # Associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

   ```
   [SwitchA-qospolicy-policy_market] classifier classifier_market behavior
   behavior_market
   ```

   # Display the sequence of issuing the traffic classes and traffic behaviors.

   ```
   [SwitchA-qospolicy-policy_market] display this
   #
   qos policy policy_market
    classifier classifier_market_mgr behavior behavior_market_mgr
   ```

```
 classifier classifier_market behavior behavior_market
#
return
[SwitchA-qospolicy-policy_market] quit
```

The output shows that the traffic class and traffic behavior for the manager office are issued first. The packets from the manager office to access the Internet are not mirrored.

4. Apply QoS policy **policy_market** to the incoming packets of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy policy_market inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B to mirror traffic from the Technical Department

1. Configure local mirroring on Switch B:

   # Create local mirroring group 1.

```
<SwitchB> system-view
[SwitchB] mirroring-group 1 local
```

   # Configure the mirroring group to monitor the incoming traffic of the port GigabitEthernet 1/0/1.

```
[SwitchB] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 inbound
```

   # Configure GigabitEthernet 1/0/2 as the monitor port of the mirroring group.

```
[SwitchB] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

2. Configure an ACL to filter the outgoing traffic from the Technical Department in working hours:

   # Create a working hour range named **work-time**, in which the working hour is from 8:30 to 18:00 on working days.

```
[SwitchB] time-range work-time 8:30 to 18:00 working-day
```

   # Create ACL 2000, and configure a rule to permit packets from 10.1.1.1 in working hours on working days.

```
[SwitchB] acl number 2000
[SwitchB-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.0 time-range work-time
[SwitchB-acl-basic-2000] quit
```

   # Apply ACL 2000 to filter the outgoing traffic on GigabitEthernet 1/0/2.

```
[SwitchB] interface GigabitEthernet1/0/2
[SwitchB-GigabitEthernet1/0/2] packet-filter 2000 outbound
[SwitchB-GigabitEthernet1/0/2] quit
```

Verifying the configuration

After the configurations are complete, display traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface

  Interface: GigabitEthernet1/0/2

  Direction: Inbound

  Policy: policy_market
   Classifier: classifier_market_mgr
     Operator: AND
```

```
    Rule(s) : If-match acl 3001
    Behavior: behavior_market_mgr
     Filter Enable: permit
  Classifier: classifier_market
    Operator: AND
    Rule(s) : If-match acl 3000
    Behavior: behavior_market
     Mirror enable:
       Mirror type: interface
       Mirror destination: GigabitEthernet1/0/3

Interface: GigabitEthernet1/0/3

Direction: Outbound

Policy: policy_servers
 Classifier: classifier_servers
   Operator: AND
   Rule(s) : If-match acl 2000
   Behavior: behavior_servers
    Mirror enable:
      Mirror type: interface
      Mirror destination: GigabitEthernet1/0/3

Interface: GigabitEthernet1/0/4

Direction: Inbound

Policy: policy_servers
 Classifier: classifier_servers
   Operator: AND
   Rule(s) : If-match acl 2000
   Behavior: behavior_servers
    Mirror enable:
      Mirror type: interface
      Mirror destination: GigabitEthernet1/0/3
```

Display information about mirroring group 1 on Switch B.

```
[SwitchB] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
    monitor port: GigabitEthernet1/0/2
```

Configuration files

- Switch A:

```
#
 time-range work-time 08:30 to 18:00 working-day
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
acl number 2001
 rule 0 permit source 14.1.1.10 0 time-range work-time
#
acl number 3000
 rule 0 permit tcp source 12.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit tcp source 12.1.1.100 0 destination-port eq www
#
traffic classifier classifier_servers operator and
 if-match acl 2000
traffic classifier classifier_fileserver operator and
 if-match acl 2001
traffic classifier classifier_market operator and
 if-match acl 3000
traffic classifier classifier_market_mgr operator and
 if-match acl 3001
#
traffic behavior behavior_servers
 mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_fileserver
 filter deny
traffic behavior behavior_market
 mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_market_mgr
 filter permit
#
qos policy policy_fileserver
 classifier classifier_fileserver behavior behavior_fileserver
qos policy policy_market
 classifier classifier_market_mgr behavior behavior_market_mgr
 classifier classifier_market behavior behavior_market
qos policy policy_servers
 classifier classifier_servers behavior behavior_servers
#
interface GigabitEthernet1/0/2
 qos apply policy policy_market inbound
#
interface GigabitEthernet1/0/3
 qos apply policy policy_servers outbound
#
interface GigabitEthernet1/0/4
 qos apply policy policy_servers inbound
```

- Switch B:

```
#
 mirroring-group 1 local
#
 time-range work-time 08:30 to 18:00 working-day
#
acl number 2000
 rule 0 permit source 10.1.1.1 0 time-range work-time
#
interface GigabitEthernet1/0/1
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 packet-filter 2000 outbound
 mirroring-group 1 monitor-port
```

MLD configuration examples

This chapter provides examples for configuring MLD to manage IPv6 multicast group membership.

General configuration restrictions and guidelines

After a Layer 2 IPv6 multicast protocol is configured on a VLAN, MLD cannot be enabled on the VLAN-interface of this VLAN.

Example: Configuring IPv6 multicast group filters

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

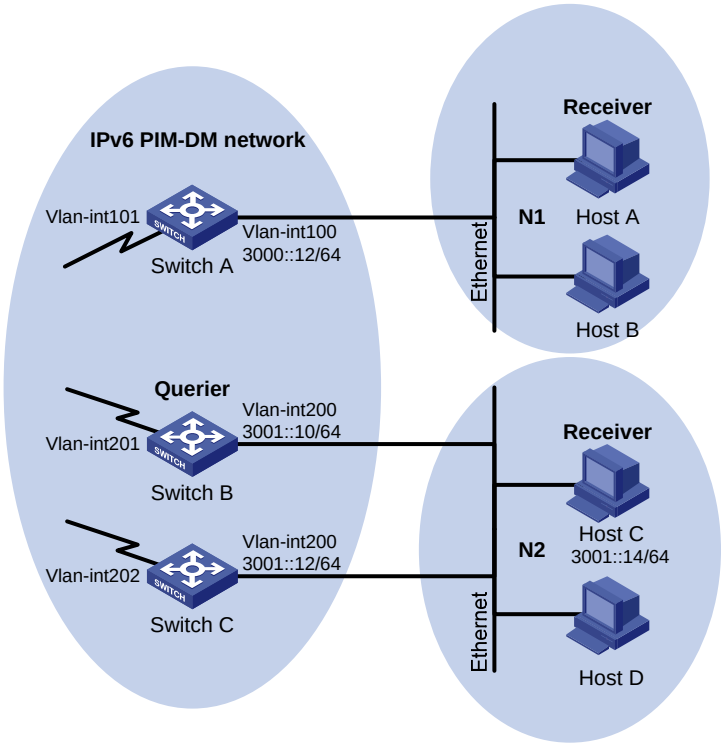
Network requirements

As shown in Figure 126:

- VOD streams are sent to receiver hosts in IPv6 multicast.
- MLDv1 runs between Switch A and N1, and between the other two switches and N2.

Configure multicast group filters on Switch B and Switch C so hosts in N2 can join only the IPv6 multicast group FF1E::101. Hosts in N1 can join any IPv6 multicast group.

Figure 126 Network diagram



Requirements analysis

To limit the MLD group range that the receivers join, create a basic IPv6 ACL and specify the IPv6 multicast group range that matches the **permit** statement in this IPv6 ACL.

Configuration restrictions and guidelines

When you configure IPv6 multicast group filters, follow these restrictions and guidelines:

- All Layer 3 switches on the same subnet must run the same version of MLD.
- To ensure consistent filtering results for the MLD-enabled switches in N2, you must configure the same IPv6 multicast group filter on these switches.

Configuration procedures

1. Enable IPv6 forwarding and assign an IPv6 address to each interface of switches in the IPv6 PIM-DM domain, as shown in Figure 126. (Details not shown.)
2. Enable OSPFv3 on all switches on the IPv6 PIM-DM network to make sure both of the following conditions exist: (Details not shown.)
   - The network layer on the IPv6 PIM-DM network is interoperable.
   - The switches can dynamically update their routing information.
3. Configure Switch A:

   # Enable IPv6 multicast routing globally,

   ```
   <SwitchA> system-view
   ```

```
[SwitchA] multicast ipv6 routing-enable
```

Enable MLD and IPv6 PIM-DM for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
```

Enable IPv6 PIM-DM for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 dm
[SwitchA-Vlan-interface101] quit
```

4. Configure Switch B:

Configure an ACL for IPv6 multicast group filtering.

```
<SwitchB> system-view
[SwitchB] acl ipv6 number 2001
[SwitchB-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchB-acl6-basic-2001] quit
```

Enable IPv6 multicast routing globally.

```
[SwitchB] multicast ipv6 routing-enable
```

Enable MLD and IPv6 PIM-DM for VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] pim ipv6 dm
```

Configure an IPv6 multicast group filter that references ACL 2001 on VLAN-interface 200, so the hosts in N2 can join only the IPv6 multicast group FF1E::101.

```
[SwitchB-Vlan-interface200] mld group-policy 2001
[SwitchB-Vlan-interface200] quit
```

Enable IPv6 PIM-DM for VLAN-interface 201.

```
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim ipv6 dm
[SwitchB-Vlan-interface201] quit
```

5. Configure Switch C:

Configure an ACL for IPv6 multicast group filtering.

```
<SwitchC> system-view
[SwitchC] acl ipv6 number 2001
[SwitchC-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchC-acl6-basic-2001] quit
```

Enable IPv6 multicast routing globally.

```
[SwitchC] multicast ipv6 routing-enable
```

Enable MLD and IPv6 PIM-DM for VLAN-interface 200.

```
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] pim ipv6 dm
```

Configure an IPv6 multicast group filter that references ACL 2001 on VLAN-interface 200, so the hosts in N2 can join only the IPv6 multicast group FF1E::101.

```
[SwitchC-Vlan-interface200] mld group-policy 2001
[SwitchC-Vlan-interface200] quit
```

Enable IPv6 PIM-DM for VLAN-interface 202.

```
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim ipv6 dm
[SwitchC-Vlan-interface202] quit
```

Verifying the configuration

1. Display information about the MLD querier in N2:

   # Display information about the MLD querier on Switch B.

```
[SwitchB] display mld interface
Interface information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958B):
   MLD is enabled
   Current MLD version is 1
   Value of query interval for MLD(in seconds): 125
   Value of other querier present interval for MLD(in seconds): 255
   Value of maximum query response time for MLD(in seconds): 10
   Querier for MLD: FE80::223:89FF:FE5F:958B (this router)
   Total 1 MLD Group reported
```

   # Display information about the MLD querier on Switch C.

```
[SwitchC] display mld interface
Interface information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958C):
   MLD is enabled
   Current MLD version is 1
   Value of query interval for MLD(in seconds): 125
   Value of other querier present interval for MLD(in seconds): 255
   Value of maximum query response time for MLD(in seconds): 10
   Querier for MLD: FE80::223:89FF:FE5F:958B
   Total 1 MLD Group reported
```

   The output shows that Switch B with the smaller IPv6 link-local address has become the MLD querier on this media-shared subnet.

2. Make Host C in N2 send the MLD reports to join IPv6 multicast groups (FF1E::101 and FF1E::102) and display information about MLD groups:

   # Display information about MLD groups on Switch B.

```
[SwitchB] display mld group
Total 1 MLD Group(s).
Interface group report information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958B):
  Total 1 MLD Group reported
   Group Address: FF1E::101
    Last Reporter: FE80::10
    Uptime: 00:01:05
    Expires: 00:03:17
```

   # Display information about MLD groups on Switch C.

```
[SwitchC] display mld group
Total 1 MLD Group(s).
```

```
Interface group report information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958C):
  Total 1 MLD Group reported
   Group Address: FF1E::101
    Last Reporter: FE80::10
    Uptime: 00:00:08
    Expires: 00:01:12
```

The output shows that only information about the IPv6 multicast group FF1E::101 is displayed on Switch B and Switch C. The configured IPv6 multicast group filters have taken effect, and the hosts in N2 can join only the IPv6 multicast group FF1E::101.

Configuration files

- Switch A:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 mld enable
 pim ipv6 dm
#
interface Vlan-interface101
 pim ipv6 dm
#
```

- Switch B:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
vlan 200 to 201
#
interface Vlan-interface200
 mld enable
 mld group-policy 2001
 pim ipv6 dm
#
interface Vlan-interface201
 pim ipv6 dm
#
```

- Switch C:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
vlan 200 to 202
#
interface Vlan-interface200
 mld enable
 mld group-policy 2001
 pim ipv6 dm
#
interface Vlan-interface202
 pim ipv6 dm
#
```

Example: Configuring MLD SSM mappings

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

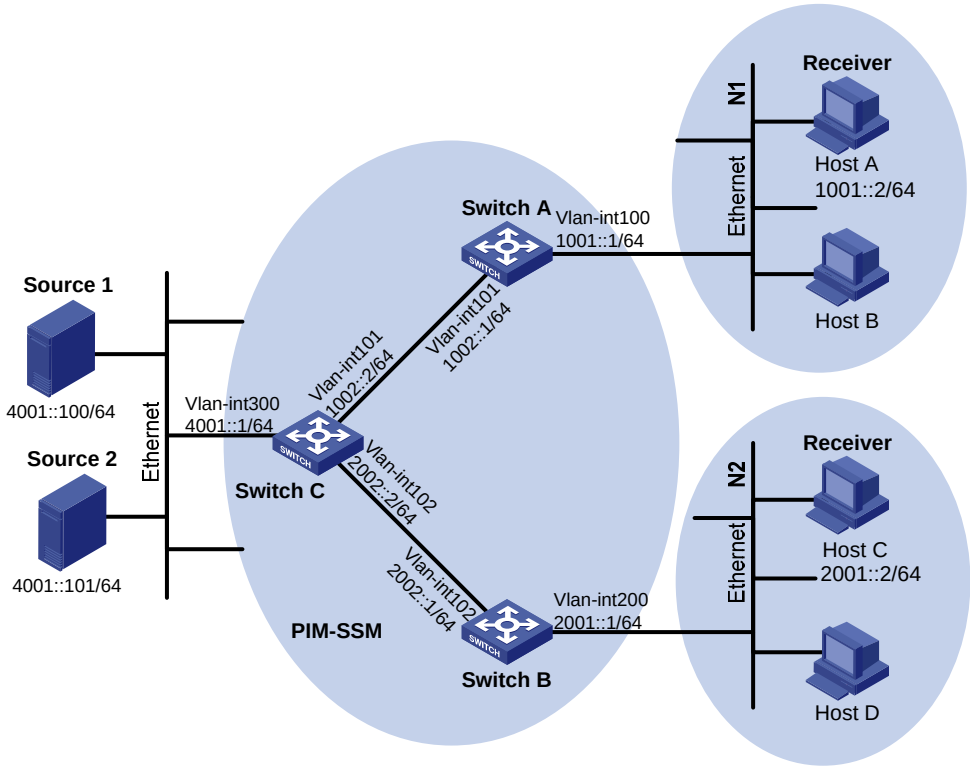
Network requirements

As shown in Figure 127:

- The IPv6 PIM-SSM network provides services for the IPv6 multicast groups in the range of FF3E::/64.
- Edge switches of N1 and N2 are running MLDv2.
- Host A and Host C support MLDv1, but do not support MLDv2.

Configure MLD SSM mappings so that Host A and Host C receive IPv6 multicast data from Source 1 and Source 2, respectively.

Figure 127 Network diagram



Configuration restrictions and guidelines

When you configure MLD SSM mappings, follow these restrictions and guidelines:

- The MLD SSM mapping does not process MLDv2 reports.
- To display information about the IPv6 multicast groups created based on the configured MLD SSM mappings, use the **display mld ssm-mapping group** command, rather than the **display mld group** command.

Configuration procedures

1. Enable IPv6 forwarding on each switch and assign an IPv6 address to each interface of switches, as shown in Figure 127. (Details not shown.)
2. Enable OSPFv3 on all switches on the IPv6 PIM-SM network to make sure both of the following conditions exist: (Details not shown.)
   - The network layer on the IPv6 PIM-SM network is interoperable.
   - The switches can dynamically update their routing information.
3. Enable IPv6 multicast routing and IPv6 PIM-SM:

   # On Switch A, enable IPv6 multicast routing, and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
```

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

Enable IPv6 multicast routing and IPv6 PIM-SM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

4. Enable MLDv2 on interfaces that connect N1 and N2:

Enable MLDv2 on VLAN-interface 100 on Switch A. (By default, the MLD version is 1.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] mld version 2
[SwitchA-Vlan-interface100] quit
```

Enable MLDv2 on Switch B in the same way Switch A is configured. (Details not shown.)

5. Specify the IPv6 SSM multicast group address range:

On Switch A, specify the IPv6 SSM multicast group address range as FF3E::/64.

```
[SwitchA] acl ipv6 number 2000
[SwitchA-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchA-acl6-basic-2000] quit
[SwitchA] pim ipv6
[SwitchA-pim6] ssm-policy 2000
[SwitchA-pim6] quit
```

Specify the same IPv6 SSM multicast group address range on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

6. Enable MLD SSM mapping and configure MLD SSM mappings:

On Switch A, enable MLD SSM mapping on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld ssm-mapping enable
[SwitchA-Vlan-interface100] quit
```

Configure an MLD SSM mapping for the IPv6 multicast source **Source 1** and IPv6 multicast groups in the range of FF3E::/64

```
[SwitchA] mld
[SwitchA-mld] ssm-mapping ff3e:: 64 4001::100
[SwitchA-mld] quit
```

On Switch B, enable MLD SSM mapping on VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld ssm-mapping enable
[SwitchB-Vlan-interface200] quit
```

Configure an MLD SSM mapping for the IPv6 multicast source **Source 2** and IPv6 multicast groups in the range of FF3E::/64.

```
[SwitchB] mld
[SwitchB-mld] ssm-mapping ff3e:: 64 4001::101
[SwitchB-mld] quit
```

Verifying the configuration

1. Make Host A and Host C send the MLDv1 reports to join the IPv6 multicast group FF3E::101.

2. Display IPv6 multicast information on Switch A:

Display the MLD SSM mapping information of the IPv6 multicast group FF3E::101.

```
[SwitchA] display mld ssm-mapping ff3e::101
 VPN-Instance: public net
 Group: FF3E::101
 Source list:
        4001::100
```

Display information about the IPv6 multicast group that was created based on the configured MLD SSM mapping.

```
[SwitchA] display mld ssm-mapping group
 Total 1 MLD SSM-mapping Group(s).
 Interface group report information of VPN-Instance: public net
 Vlan-interface100(FE80::223:89FF:FE5F:958A):
  Total 1 MLD SSM-mapping Group reported
    Group Address: FF3E::101
    Last Reporter: FE80::10
    Uptime: 00:02:04
    Expires: off
```

Display the IPv6 PIM routing table.

```
[SwitchA] display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (4001::100, FF3E::101)
     Protocol: pim-ssm, Flag:
     UpTime: 00:13:25
     Upstream interface: Vlan-interface101
         Upstream neighbor: FE80::223:89FF:FE5F:958C
         RPF prime neighbor: FE80::223:89FF:FE5F:958C
     Downstream interface(s) information:
       Total number of downstreams: 1
         1: Vlan-interface100
                 Protocol: mld, UpTime: 00:13:25, Expires: -
```

3. Display IPv6 multicast information on Switch B:

Display the MLD SSM mapping information of the IPv6 multicast group FF3E::101.

```
[SwitchB] display mld ssm-mapping ff3e::101
 VPN-Instance: public net
 Group: FF3E::101
 Source list:
        4001::101
```

Display information about the IPv6 multicast group that was created based on the configured MLD SSM mapping.

```
[SwitchB] display mld ssm-mapping group
 Total 1 MLD SSM-mapping Group(s).
 Interface group report information of VPN-Instance: public net
 Vlan-interface200(FE80::223:89FF:FE5F:958B):
  Total 1 MLD SSM-mapping Group reported
```

```
    Group Address: FF3E::101
    Last Reporter: FE80::13
    Uptime: 00:01:26
    Expires: off
```

Display the IPv6 PIM routing table.

```
[SwitchB] display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

 (4001::101, FF3E::101)
     Protocol: pim-ssm, Flag:
     UpTime: 00:12:16
     Upstream interface: Vlan-interface102
         Upstream neighbor: FE80::223:89FF:FE5F:958C
         RPF prime neighbor: FE80::223:89FF:FE5F:958C
     Downstream interface(s) information:
       Total number of downstreams: 1
         1: Vlan-interface200
                 Protocol: mld, UpTime: 00:05:21, Expires: -
```

The output shows that:

- After an MLD SSM mapping is configured on Switch A, Switch A translates (::,FF3E::101) into (4001::100, FF3E::101), so Host A can receive IPv6 multicast data only from Source 1.
- After an MLD SSM mapping is configured on Switch B, Switch B translates (::,FF3E::101) into (4001::100, FF3E::101), so Host C can receive IPv6 multicast data only from Source 2.

Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 mld version 2
 mld ssm-mapping enable
 pim ipv6 sm
#
interface Vlan-interface101
```

```
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
mld
 ssm-mapping ff3e:: 64 4001::100
#
pim ipv6
 ssm-policy 2000
#
```

- Switch B:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface200
 ipv6 address 2001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 mld version 2
 mld ssm-mapping enable
 pim ipv6 sm
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
mld
 ssm-mapping ff3e:: 64 4001::101
#
pim ipv6
```

```
 ssm-policy 2000
#
```

- Switch C:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface102
 ipv6 address 2002::2/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface300
 ipv6 address 4001::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
pim ipv6
 ssm-policy 2000
#
```

MLD snooping configuration examples

This chapter provides examples for configuring MLD snooping to manage and control IPv6 multicast group forwarding at Layer 2.

General configuration restrictions and guidelines

MLD snooping cannot be run on a VLAN whose VLAN interface is running a Layer 3 multicast protocol.

Example: Configuring an MLD snooping multicast group filter

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

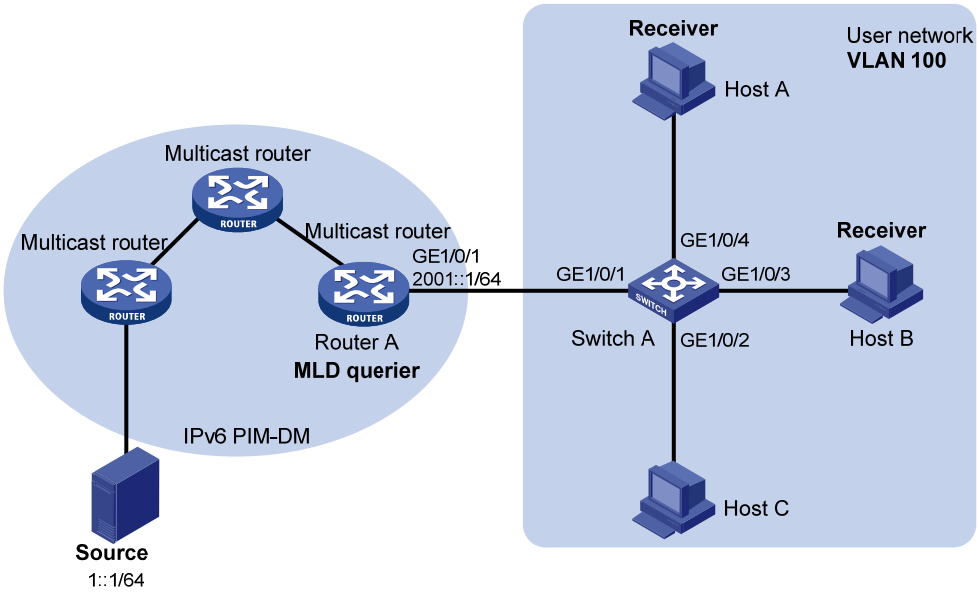
Network requirements

As shown in Figure 128, user network VLAN 100 is connected to the MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.

Users in VLAN 100 want to receive IPv6 multicast packets from the multicast source at 1::1/64.

Configure an MLD snooping multicast group filter on Switch A so hosts in VLAN 100 can join only multicast packets destined for multicast group FF1E::101.

Figure 128 Network diagram



Requirements analysis

To prevent the hosts in VLAN 100 from receiving multicast packets from other IPv6 multicast groups, enable dropping unknown IPv6 multicast packets for the VLAN 100.

To configure an MLD snooping multicast group filter to allow hosts in VLAN 100 to join only IPv6 multicast group FF1E::101, perform the following configuration:

- Create a basic IPv6 ACL.
- Add a rule that permits only packets from FF1E::101.

Configuration restrictions and guidelines

If the IPv6 ACL specified for the MLD snooping multicast group filter does not exist or has no rule, the filter will filter out packets from any multicast group.

Configuration procedures

Enable IPv6 forwarding on the switch. (Details not shown.)

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN,

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable MLD snooping and dropping unknown IPv6 multicast packets for VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
```

```
[SwitchA-vlan100] mld-snooping drop-unknown
[SwitchA-vlan100] quit
```

Configure an IPv6 multicast group filter so hosts in VLAN 100 can join only IPv6 multicast group FF1E::101.

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA-mld-snooping] group-policy 2001 vlan 100
[SwitchA-mld-snooping] quit
```

Verifying the configuration

1. Make Host A send MLD reports with the multicast group address FF1E::101.
2. Make Host B send MLD reports with the multicast group address FF1E::102.
3. Display detailed information about MLD snooping groups on Switch A:

```
[SwitchA] display mld-snooping group verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x00000000000000001)
    Router port(s):total 1 port.
            GE1/0/1              (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:FF1E::101
        (::, FF1E::101):
          Attribute:    Host Board
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port.
            GE1/0/4              (D)
    MAC group(s):
      MAC group address: 3333-0000-0101
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port.
            GE1/0/4
```

The output shows that Switch A has only the entry for IPv6 multicast group FF1E::101. The filter is functioning.

Configuration files

Switch A:

```
#
 ipv6
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
 mld-snooping
 group-policy 2001 vlan 100
#
vlan 100
 mld-snooping enable
 mld-snooping drop-unknown
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Configuring MLD snooping static ports

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 129, user network VLAN 100 is connected to the MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.

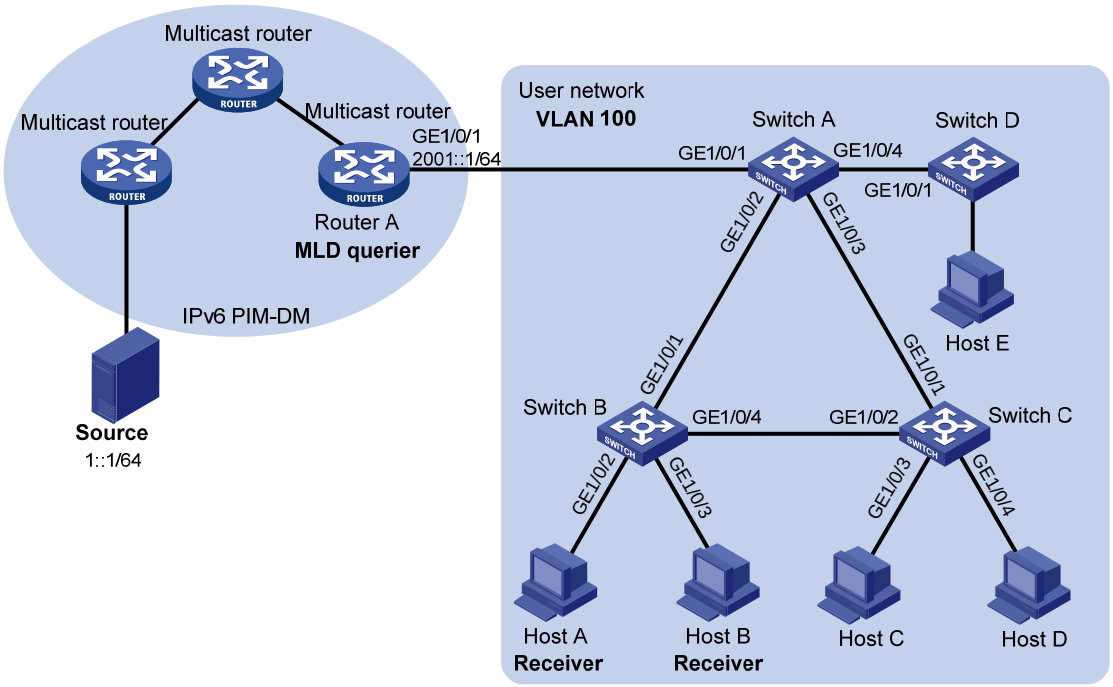
Users in VLAN 100 want to receive the multicast packets from the multicast source at 1::1/64. In the user network, Switch A, Switch B, and Switch C form a ring and are running STP to avoid loops.

Enable the function of dropping unknown IPv6 multicast packets. This feature prevents unknown IPv6 multicast packets from being broadcasted in the user network.

Configure MLD snooping static member ports and MLD snooping static router ports to achieve the following goals:

- Host A and Host B receive multicast packets for a fixed IPv6 multicast group (FF1E::101).
- IPv6 multicast packets can switch from one failed path between Switch A and Switch B to the other path immediately after the new path comes up and becomes stable.

Figure 129 Network diagram



Requirements analysis

Configure the ports on the switches that are connected to the hosts as MLD snooping static member ports of the IPv6 multicast group. This configuration enables hosts to receive multicast packets for a fixed IPv6 multicast group.

After an STP switching occurs and the new path becomes stable, at least one MLD query/response exchange is required before the new path can forward IPv6 multicast packets. Configure all ports that might become multicast packet outbound ports on the switches in the ring as MLD snooping static router ports. This configuration makes the ports forward IPv6 multicast packets through the new path immediately after the new path comes up.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Configure Switch A:

   # Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
```

```
[SwitchA-mld-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable MLD snooping for VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as MLD snooping static router ports.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

3. Configure Switch B:

Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable MLD snooping for VLAN 100.

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as MLD snooping static member ports of the IPv6 multicast group FF1E::101.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
```

4. Configure Switch C:

Enable MLD snooping globally.

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/4
```

Enable MLD snooping for VLAN 100.

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

Configure GigabitEthernet 1/0/2 as an MLD snooping static router port.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Make Host A and Host B send MLD reports with the multicast address FF1E::101 and display MLD snooping information:

Display detailed information about MLD snooping forwarding entries for VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x00000000000000001)
    Router port(s):total 3 port.
            GE1/0/1                 (D)
            GE1/0/2                 (S)
            GE1/0/3                 (S)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address: FF1E::101
        (::, FF1E::101):
          Attribute:    Host Board
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port.
            GE1/0/2                 (D)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port unit board: Mask(0x00000000000000001)
          Host port(s):total 1 port.
            GE1/0/2
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet1/0/3 on Switch A are MLD snooping static router ports.

Display detailed information about MLD snooping groups for VLAN 100 on Switch B.

```
[SwitchB] display mld-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
         GE1/0/2              (D)
  IP group(s):the following ip group(s) match to one mac group.
    IP group address: FF1E::101
      (::, FF1E::101):
        Attribute:    Host Board
        Host port unit board: Mask(0x00000000000000001)
        Host port(s):total 2 port.
          GE1/0/2              (S)
          GE1/0/3              (S)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port unit board: Mask(0x00000000000000001)
        Host port(s):total 2 port.
          GE1/0/2
          GE1/0/3
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch B are MLD snooping static router ports for the IPv6 multicast group.

Configuration files

- Switch A:

```
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
```

```
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch B:

```
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 mld-snooping static-group ff1e::101 vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping static-group ff1e::101 vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch C:

```
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Configuring the MLD snooping querier

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

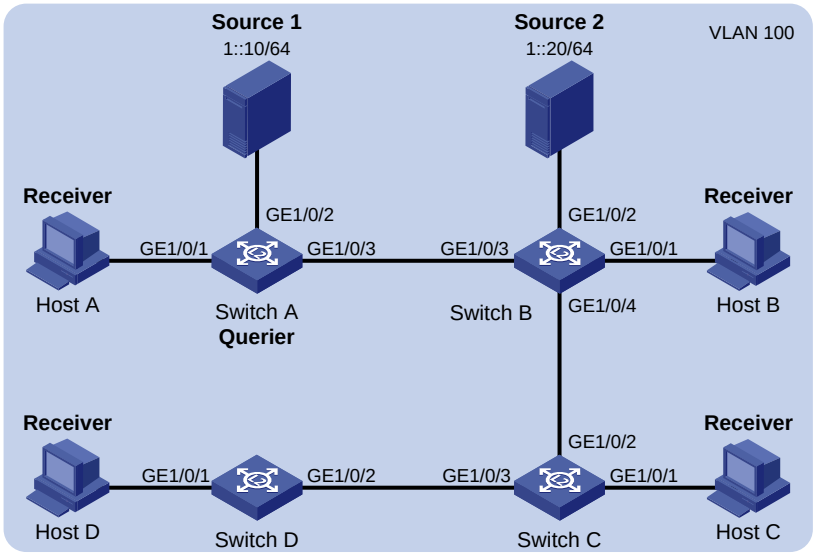
Network requirements

The network shown in Figure 130 is a Layer 2-only network.

- Source 1 and Source 2 send multicast packets to multicast groups FF1E::101 and FF1E::102, respectively.
- Host A and Host C are receivers of multicast group FF1E::101.
- Host B and Host D are receivers of multicast group FF1E::102.

Configure an MLD snooping querier so the receivers receive their respective multicast packets.

Figure 130 Network diagram



Requirements analysis

Configure the switch that is nearer to the multicast sources (Switch A, in this example) as the MLD snooping querier. This configuration ensures that all devices between the multicast sources and the receivers establish and maintain Layer 2 multicast forwarding entries.

Configuration procedures

1. Enable IPv6 forwarding on each switch. (Details not shown.)
2. Configure Switch A:

   # Enable MLD snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] mld-snooping
   [SwitchA-mld-snooping] quit
   ```

   # Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100.

   ```
   [SwitchA] vlan 100
   [SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
   ```

   # Enable MLD snooping and the MLD snooping querier feature for VLAN 100.

   ```
   [SwitchA-vlan100] mld-snooping enable
   [SwitchA-vlan100] mld-snooping querier
   [SwitchA-vlan100] quit
   ```

3. Configure Switch B:

   # Enable MLD snooping globally.

   ```
   <SwitchB> system-view
   [SwitchB] mld-snooping
   [SwitchB-mld-snooping] quit
   ```

   # Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

   ```
   [SwitchB] vlan 100
   [SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
   ```

   # Enable MLD snooping for VLAN 100.

   ```
   [SwitchB-vlan100] mld-snooping enable
   [SwitchB-vlan100] quit
   ```

4. Configure Switch C and Switch D in the same way as Switch B is configured. (Details not shown.)

Verifying the configuration

After the configuration is completed, use the **display mld-snooping statistics** command on any switch to display statistics for the MLD messages that are learned by MLD snooping.

On Switch B, display statistics for the MLD messages that are learned by MLD snooping.

```
[SwitchB-vlan100] display mld-snooping statistics
  Received MLD general queries:96.
  Received MLDv1 specific queries:0.
  Received MLDv1 reports:105.
  Received MLD dones:0.
  Sent     MLDv1 specific queries:0.
  Received MLDv2 reports:0.
  Received MLDv2 reports with right and wrong records:0.
  Received MLDv2 specific queries:0.
  Received MLDv2 specific sg queries:0.
```

```
Sent     MLDv2 specific queries:0.
Sent     MLDv2 specific sg queries:0.
Received error MLD messages:0.
```

The output shows that an MLD snooping querier configured in a Layer 2 network can send MLD queries in the network.

Configuration files

- Switch A:

```
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
 mld-snooping querier
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
```

- Switch B:

```
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch C and Switch D: (Similar to the configuration on Switch B. Details not shown.)

Example: Configuring MLD snooping proxying

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

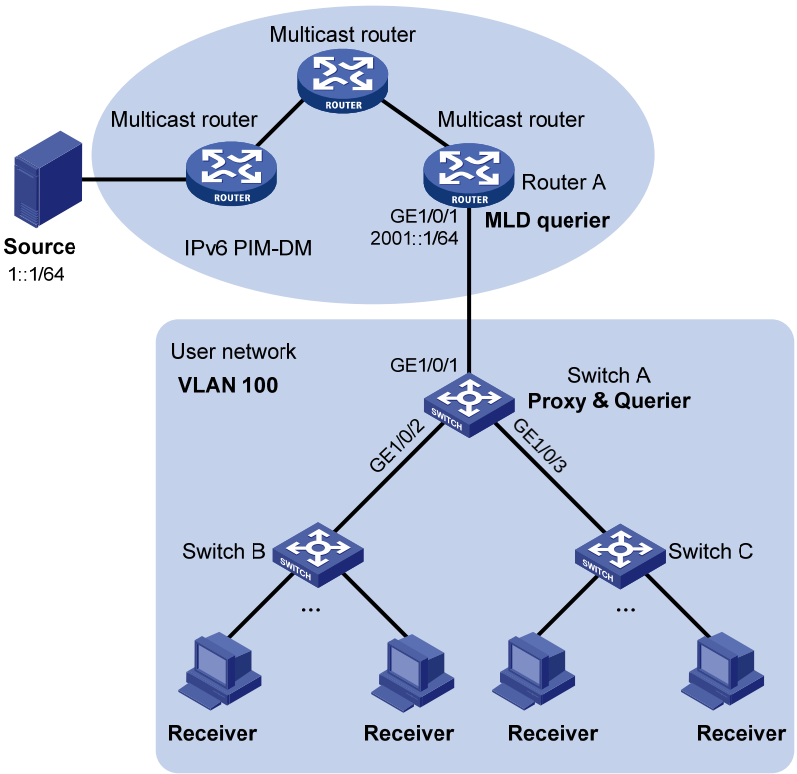
Network requirements

As shown in Figure 131, user network VLAN 100 is connected to the MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.

Many receivers in the VLAN frequently join or leave the multicast group, sending large amounts of MLD reports and done messages.

Enable MLD snooping on the switches in the user network. Configure MLD snooping proxying so the MLD querier does not need to process large amounts of MLD reports and done messages.

Figure 131 Network diagram



Requirements analysis

To reduce the number of MLD reports and done messages sent to the MLD querier, configure the MLD snooping proxying on the switch that is nearest to the MLD querier (Switch A, in this example).

Configuration restrictions and guidelines

Before configuring MLD snooping proxying, enable MLD snooping globally and specifically for the VLAN.

Configuration procedures

1. Enable IPv6 forwarding on each switch. (Details not shown.)
2. Configure Switch A:

   # Enable MLD snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] mld-snooping
   [SwitchA-mld-snooping] quit
   ```

   # Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the VLAN.

   ```
   [SwitchA] vlan 100
   [SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
   ```

   # Enable MLD snooping and MLD snooping proxying for VLAN 100.

   ```
   [SwitchA-vlan100] mld-snooping enable
   [SwitchA-vlan100] mld-snooping proxying enable
   ```

   # Configure the source IPv6 addresses for the proxy to use for MLD reports and done messages.

   ```
   [SwitchA-vlan100] mld-snooping report source-ip fe80:0:0:1::1
   [SwitchA-vlan100] mld-snooping done source-ip fe80:0:0:1::1
   [SwitchA-vlan100] quit
   ```

3. Configure Switch B and Switch C: (Details not shown.)
   a. Create VLAN 100 and assign ports that are connected to the receiver hosts to the VLAN.
   b. Enable MLD snooping for the VLAN.

Verifying the configuration

Make the hosts in the user network send MLD reports with the multicast address FF1E::101, and display MLD multicast group information:

Display MLD multicast group information on Router A.

```
[RouterA] display mld group
Total 1 MLD Group(s).
Interface group report information of VPN-Instance: public net
 GigabitEthernet1/0/1(FE80::200:FCFF:FE00:7507):
  Total 1 MLD Group reported
   Group Address: FF1E::101
    Last Reporter: FE80:0:0:1::1
```

```
    Uptime: 00:00:03
    Expires: 00:04:17
```

The output shows that the last member report was from the source IPv6 address for the MLD snooping proxy to use for MLD reports. Switch A has sent MLD reports to the MLD querier on behalf of receiver hosts.

Configuration files

```
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
 mld-snooping proxying enable
 mld-snooping report source-ip fe80:0:0:1::1
 mld-snooping done source-ip fe80:0:0:1::1
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
```

MPLS L2VPN configuration examples

This document provides MPLS L2VPN configuration examples.

MPLS L2VPN is an MPLS-based Layer 2 VPN technology. It offers Layer 2 VPN services over an MPLS network. MPLS L2VPN can transparently transmit Layer 2 data for different data link layer protocols.

Table 13 MPLS L2VPN modes and application scenarios

MPLS L2VPN mode	Applies to this scenario
CCC	A few customer sites and a few backbone devices exist.
SVC	A few customer sites exist, and a lot of backbone devices exist.
Layer 3 interface-based Martini	A lot of customer sites exist and a customer site connected to a PE's port uses the same VC connection.
Service instance-based Martini	A lot of customer sites exist and users in a customer site connected to a PE's port use different VC connections.
Kompella	A lot of customer sites exist and new sites will be connected to the backbone through new PEs.

General configuration restrictions and guidelines

Hardware requirements

To support MPLS L2VPN, the HP 7500 Switch Series must use an EB, SD, LSQ1QGS4SC, or LSQ1QGC4SC card, and use the ports on the card to connect to the user network and carrier network.

Example: Configuring CCC MPLS L2VPN

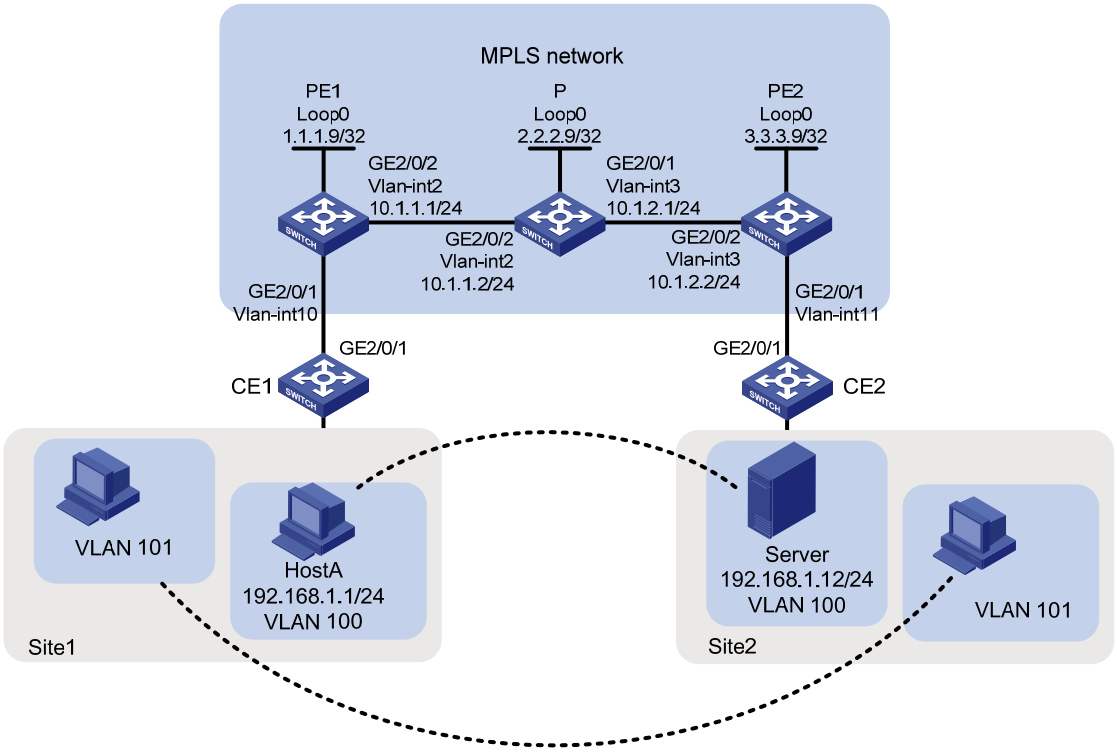
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 132, configure CCC MPLS L2VPN so the two sites in the same VLAN can communicate with each other at Layer 2.

Figure 132 Network diagram



Configuration restrictions and guidelines

When you configure CCC MPLS L2VPN, follow these restrictions and guidelines:

- On the two PEs, specify the incoming and outgoing labels for the CCC connection instead of configuring static LSPs. The incoming label is exclusive to the CCC connection.
- On the P device, configure a static LSP for each direction of the CCC connection.

Configuration procedures

Configuring CE 1

Create VLAN 100 and VLAN 101.

```
<CE1> system-view
[CE1] vlan 100 to 101
```

Configure the uplink port GigabitEthernet 2/0/1 as a trunk port.

```
[CE1] interface GigabitEthernet 2/0/1
[CE1-GigabitEthernet2/0/1] port link-type trunk
```

Configure the port to permit tagged packets from VLAN 100 and VLAN 101.

```
[CE1-GigabitEthernet2/0/1] port trunk permit vlan 100 101
```

Configuring PE 1

1. Configure an LSR ID, and enable MPLS globally.

```
<PE1> system-view
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
```

2. Enable MPLS L2VPN globally.

```
[PE1] l2vpn
[PE1-l2vpn] mpls l2vpn
[PE1-l2vpn] quit
```

3. Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE1] vlan 2
[PE1-vlan2] port GigabitEthernet 2/0/2
[PE1-vlan2] quit
```

4. Configure VLAN-interface 2, and enable MPLS on it.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] quit
```

5. Create VLAN 10, assign GigabitEthernet 2/0/1 to VLAN 10, and create VLAN-interface 10.

```
[PE1] vlan 10
[PE1-vlan10] port GigabitEthernet 2/0/1
[PE1-vlan10] quit
[PE1] interface Vlan-interface 10
[PE1-Vlan-interface10] quit
```

6. Create a remote CCC connection from CE 1 to CE 2.

```
[PE1] ccc ce1-ce2 interface vlan-interface 10 in-label 100 out-label 200 nexthop
10.1.1.2
```

Configuring P

1. Configure an LSR ID, and enable MPLS globally.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
```

2. Create VLAN 3, and assign GigabitEthernet 2/0/1 to the VLAN.

```
[P] vlan3
[P-vlan3] port GigabitEthernet2/0/1
[P-vlan3] quit
```

3. # Configure VLAN-interface 3, and enable MPLS on it.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] mpls
[P-Vlan-interface3] quit
```

4. Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[P] vlan2
[P-vlan2] port GigabitEthernet2/0/2
[P-vlan2] quit
```

5. Configure VLAN-interface 2, and enable MPLS on it.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] quit
```

6. Create a static LSP for forwarding packets from PE 1 to PE 2.

```
[P] static-lsp transit pe1_pe2 incoming-interface vlan-interface 2 in-label 200
nexthop 10.1.2.2 out-label 201
```

7. Create a static LSP for forwarding packets from PE 2 to PE 1.

```
[P] static-lsp transit pe2_pe1 incoming-interface vlan-interface 3 in-label 101
nexthop 10.1.1.1 out-label 100
```

Configuring PE 2

1. Configure an LSR ID, and enable MPLS globally.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
```

2. Enable MPLS L2VPN globally.

```
[PE2] mpls l2vpn
```

3. Create VLAN 11, and assign GigabitEthernet 2/0/1 to the VLAN.

```
[PE2] vlan 11
[PE2-vlan11] port GigabitEthernet 2/0/1
[PE2-vlan11] quit
```

4. Create VLAN-interface 11.

```
[PE2] interface vlan-interface 11
[PE2-Vlan-interface11] quit
```

5. Create VLAN 3, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE2] vlan 3
[PE2-vlan3] port GigabitEthernet 2/0/2
[PE2-vlan3] quit
```

6. Configure VLAN-interface 3, and enable MPLS on it.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] quit
```

7. Create a remote CCC connection from CE 2 to CE 1.

```
[PE2] ccc ce2-ce1 interface vlan-interface 11 in-label 201 out-label 101 nexthop
10.1.2.1
```

Configuring CE 2

Create VLAN 100 and VLAN 101.

```
<CE2> system-view
[CE2] vlan 100 to 101
```

Configure the uplink port GigabitEthernet 2/0/1 as a trunk port.

```
[CE2] interface GigabitEthernet 2/0/1
[CE2-GigabitEthernet2/0/1] port link-type trunk
```

Configure the port to permit tagged packets from VLAN 100 and VLAN 101.

```
[CE2-GigabitEthernet2/0/1] port trunk permit vlan 100 101
```

Verifying the configuration

Display CCC connection information on PE 1. The output shows that a remote CCC connection has been established.

```
[PE1] display ccc
    Total  ccc vc          : 1
    Local  ccc vc          : 0,  0 up
    Remote ccc vc          : 1,  1 up
 ***Name                   : ce1-ce2
    Type                   : remote
    State                  : up
    Intf                   : Vlan-interface10 (up)
    In-label               : 100
    Out-label              : 200
    Nexthop                : 10.1.1.2
```

Ping Host A from the server or ping the server from Host A. If the ping operation succeeds, you can conclude that the MPLS L2VPN has been established.

Configuration files

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 3
#
mpls
#
l2vpn
 mpls l2vpn
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
```

```
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface Vlan-interface10
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2
#
 ccc ce1-ce2 interface Vlan-interface10 in-label 100 out-label 200 nexthop 10.1.1.2
```

- P:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 10
#
mpls
#
l2vpn
 mpls l2vpn
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet2/0/2
```

```
 port link-mode bridge
 port access vlan 2
#
static-lsp transit pe1_pe2 incoming-interface vlan-interface 2 in-label 200 nexthop
10.1.2.2 out-label 201
static-lsp transit pe2_pe1 incoming-interface vlan-interface 3 in-label 101 nexthop
10.1.1.1 out-label 100
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 11
#
mpls
#
l2vpn
 mpls l2vpn
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
#
interface Vlan-interface11
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 3
#
ccc ce2-ce1 interface vlan-interface 11 in-label 201 out-label 101 nexthop 10.1.2.1
```

Example: Configuring SVC MPLS L2VPN

Applicable product matrix

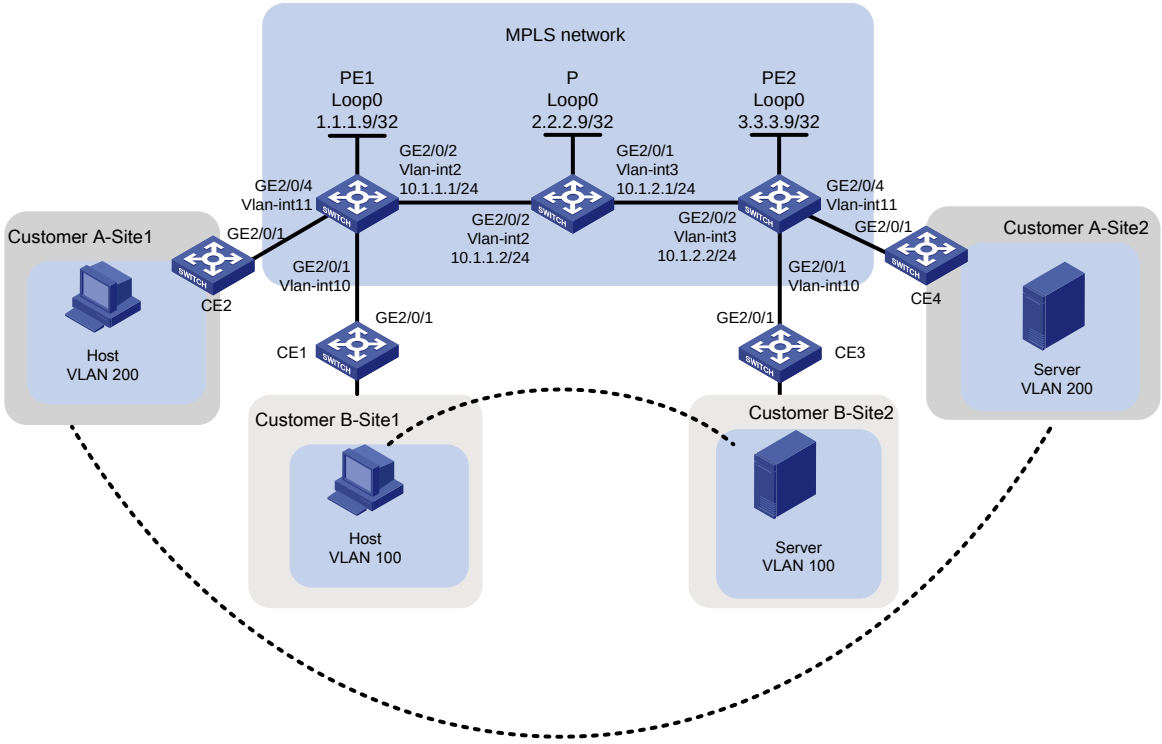
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 133, the MPLS network provides L2VPN services for two customers. Each customer has two fixed sites.

Configure SVC MPLS L2VPN so the hosts in different sites of a customer can communicate with each other at Layer 2 in the same VLAN.

Figure 133 Network diagram



Requirements analysis

To identify the CEs of different customers, configure VC IDs on each PE.

Configuration restrictions and guidelines

Before you configure SVC MPLS L2VPN, determine the VC IDs for each PE and ensure user data security.

When you configure an SVC on a PE, make sure the incoming label is identical with the outgoing label configured on the peer PE.

Configuration procedures

Configuring CEs

On each CE, configure the interface that connects to the PE to permit tagged packets from the customer VLAN. This example uses CE 1.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface GigabitEthernet 2/0/1
[CE1-GigabitEthernet2/0/1] port link-type trunk
[CE1-GigabitEthernet2/0/1] port trunk permit vlan 100
```

Configuring PE 1

1. Create VLANs and the corresponding VLAN interfaces:

   # Create VLAN 10, assign GigabitEthernet 2/0/1 to VLAN 10, and create VLAN-interface 10.

   ```
   <PE1> system-view
   [PE1] vlan 10
   [PE1-vlan10] port GigabitEthernet 2/0/1
   [PE1-vlan10] quit
   [PE1] interface Vlan-interface 10
   [PE1-Vlan-interface10] quit
   ```

   # Create VLAN 11, assign GigabitEthernet 2/0/4 to VLAN 11, and create VLAN-interface 11.

   ```
   [PE1] vlan 11
   [PE1-vlan11] port GigabitEthernet 2/0/4
   [PE1-vlan11] quit
   [PE1] interface Vlan-interface 11
   [PE1-Vlan-interface11] quit
   ```

2. Configure LDP to generate the outer label:

   # Configure an LSR ID, and enable MPLS globally.

   ```
   [PE1] interface loopback 0
   [PE1-LoopBack0] ip address 1.1.1.9 32
   [PE1-LoopBack0] quit
   [PE1] mpls lsr-id 1.1.1.9
   [PE1] mpls
   ```

   # Allow all routing entries to trigger the establishment of LSPs.

   ```
   [PE1-mpls] lsp-trigger all
   [PE1-mpls] quit
   ```

   # Enable MPLS L2VPN and LDP globally.

   ```
   [PE1] l2vpn
   [PE1-l2vpn] mpls l2vpn
   [PE1-l2vpn] quit
   [PE1] mpls ldp
   [PE1-mpls-ldp] quit
   ```

   # Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

   ```
   [PE1] vlan 2
   [PE1-vlan2] port GigabitEthernet 2/0/2
   ```

```
[PE1-vlan2] quit
```

Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

Configure OSPF on PE 1 for establishing LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

3. Configure VC IDs for the CEs:

Create an SVC to PE 2 on the interface that connects to CE 1. Specify the outgoing VC label as 101 and the incoming VC label as 100.

```
[PE1] interface vlan-interface 10
[PE1-Vlan-interface10] mpls static-l2vc destination 3.3.3.9 transmit-vpn-label 101
receive-vpn-label 100
[PE1-Vlan-interface10] quit
```

Create an SVC to PE 2 on the interface that connects to CE 2. Specify the outgoing VC label as 201 and the incoming VC label as 200.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] mpls static-l2vc destination 3.3.3.9 transmit-vpn-label 201
receive-vpn-label 200
[PE1-Vlan-interface11] quit
```

Configuring P

1. Configure an LSR ID, and enable MPLS globally.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] mpls lsr-id 2.2.2.9
[P] mpls
```

2. Allow all routing entries to trigger the establishment of LSPs.

```
[P-mpls] lsp-trigger all
[P-mpls] quit
```

3. Enable LDP globally.

```
[P] mpls ldp
[P-mpls-ldp] quit
```

4. Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[P] vlan2
[P-vlan2] port GigabitEthernet2/0/2
[P-vlan2] quit
```

5. Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
```

6. Create VLAN 3, and assign GigabitEthernet 2/0/1 to the VLAN.

```
[P] vlan3
[P-vlan3] port GigabitEthernet2/0/1
[P-vlan3] quit
```

7. Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

8. Configure OSPF on P for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.1 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configuring PE 2

1. Create VLANs and the corresponding VLAN interfaces:

   # Create VLAN 10, assign GigabitEthernet 2/0/1 to VLAN 10, and create VLAN-interface 10.

```
<PE2> system-view
[PE2] vlan 10
[PE2-vlan10] port GigabitEthernet 2/0/1
[PE2-vlan10] quit
[PE2] interface Vlan-interface 10
[PE2-Vlan-interface10] quit
```

   # Create VLAN 11, assign GigabitEthernet 2/0/4 to VLAN 11, and create VLAN-interface 11.

```
[PE2] vlan 11
[PE2-vlan11] port GigabitEthernet 2/0/4
[PE2-vlan11] quit
[PE2] interface Vlan-interface 11
[PE2-Vlan-interface11] quit
```

2. Configure LDP to generate the outer label:

   # Configure the LSR, and enable MPLS globally.

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
```

   # Allow all routing entries to trigger the establishment of LSPs.

```
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
```

Enable MPLS L2VPN and LDP globally.

```
[PE2] l2vpn
[PE2-l2vpn] mpls l2vpn
[PE2-l2vpn] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

Create VLAN 3, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE2] vlan 3
[PE2-vlan3] port GigabitEthernet 2/0/2
[PE2-vlan3] quit
```

Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.2 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

3. Configure VC IDs for the CEs:

Create an SVC to PE 1 on the interface that connects to CE 3. Specify the outgoing VC label as 100 and incoming VC label as 101.

```
[PE2] interface vlan-interface 10
[PE2-Vlan-interface10] mpls static-l2vc destination 1.1.1.9 transmit-vpn-label 100
receive-vpn-label 101
[PE2-Vlan-interface10] quit
```

Create an SVC to PE 1 on the interface that connects to CE 2. Specify the outgoing VC label as 200 and incoming VC label as 201.

```
[PE2] interface vlan-interface 11
[PE2-Vlan-interface11] mpls static-l2vc destination 1.1.1.9 transmit-vpn-label 200
receive-vpn-label 201
[PE2-Vlan-interface11] quit
```

Verifying the configuration

Display SVC information on PE 1. The output shows that two VCs have been established.

```
[PE1] display mpls static-l2vc
Total connections:  2,  2 up,  0 down
ce-intf             state destination     tr-label  rcv-label tnl-policy
Vlan10              up    3.3.3.9         101       100       default
Vlan11              up    3.3.3.9         201       200       default
```

Verify that the host and the server of the same customer but in different sites can reach other. If they can, you can conclude that the MPLS L2VPN has been established.

Configuration files

- PE1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 10 to 11
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface10
 mpls static-l2vc destination 3.3.3.9 transmit-vpn-label 101 receive-vpn-label 100
#
interface Vlan-interface11
 mpls static-l2vc destination 3.3.3.0 transmit-vpn-label 201 receive-vpn-label 200
#
interface GigabitEthernet2/0/1
 port access vlan 10
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
interface GigabitEthernet2/0/4
 port access vlan 11
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
```

- P:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 3
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port access vlan 3
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
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
  network 2.2.2.9 0.0.0.0
```

- PE2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 10 to 11
#
mpls
 lsp-trigger all
#
```

```
l2vpn
 mpls l2vpn
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface10
 mpls static-l2vc destination 1.1.1.9 transmit-vpn-label 100 receive-vpn-label 101
#
interface Vlan-interface11
 mpls static-l2vc destination 1.1.1.9 transmit-vpn-label 200 receive-vpn-label 201
#
interface GigabitEthernet2/0/1
 port access vlan 10
#
interface GigabitEthernet2/0/2
 port access vlan 3
#
interface GigabitEthernet2/0/4
 port access vlan 11
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
```

Example: Configuring Layer 3 interface-based Martini MPLS L2VPN

Applicable product matrix

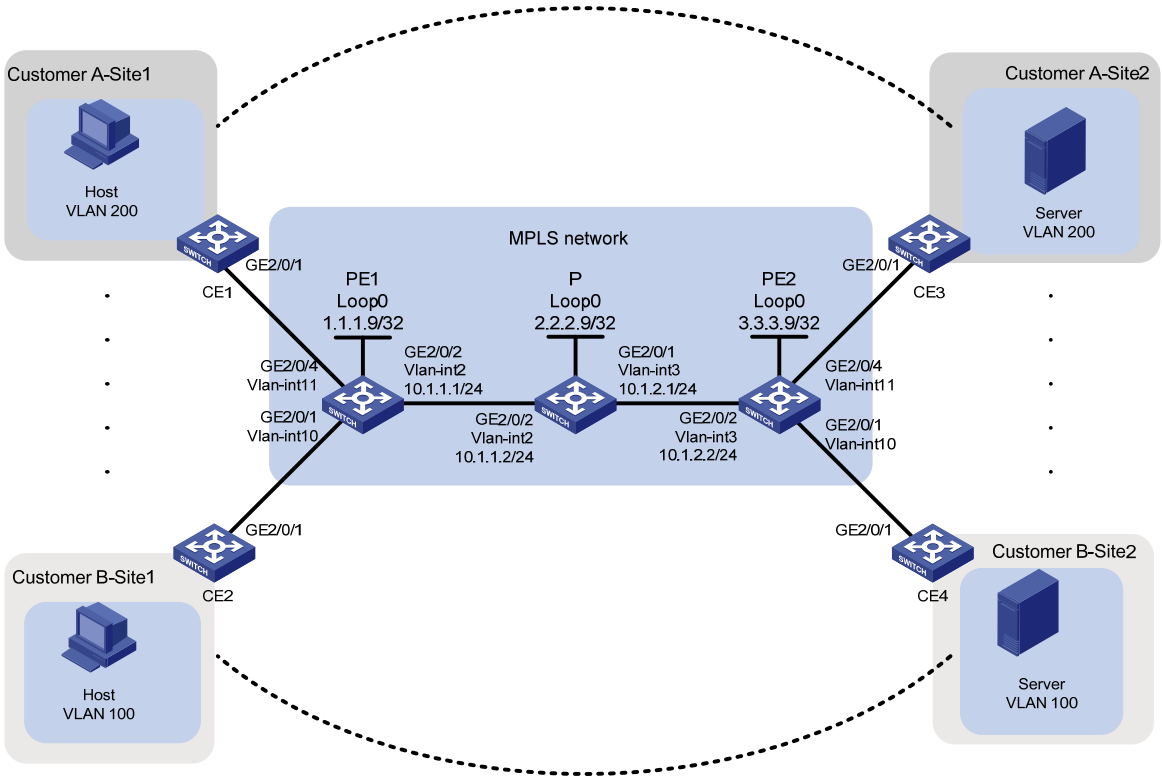
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 134, the MPLS network provides L2VPN services for two customers. The customers will add or remove VPN sites.

Configure Layer 3 interface-based Martini MPLS L2VPN so the MPLS network can adapt to changes without needing complex configurations. In this example, the sites of Customer A are added first, and then the sites of Customer B are added with simple configurations.

Figure 134 Network diagram



Requirements analysis

To exchange inner labels between PEs, configure the two PEs as LDP peers.

To identify CEs on a PE, configure a unique VC ID for each CE. Be sure to configure the same VC IDs on the two PEs to ensure data security.

Configuration procedures

Configuring CEs

On each CE, configure the interface that connects to the PE to permit tagged packets from the customer VLAN. This example uses CE 1.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface GigabitEthernet 2/0/1
```

```
[CE1-GigabitEthernet2/0/1] port link-type trunk
[CE1-GigabitEthernet2/0/1] port trunk permit vlan 200
```

Configuring PE 1

1. Create VLAN 11, assign GigabitEthernet 2/0/4 to VLAN 11, and create VLAN-interface 11.

```
<PE> system-view
[PE1] vlan 11
[PE1-vlan11] port GigabitEthernet 2/0/4
[PE1-vlan11] quit
[PE1] interface Vlan-interface 11
[PE1-Vlan-interface11] quit
```

2. Configure LDP to generate the outer label:

Configure an LSR ID, and enable MPLS globally.

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
```

Allow all routing entries to trigger the establishment of LSPs.

```
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
```

Enable MPLS L2VPN and LDP globally.

```
[PE1] l2vpn
[PE1-l2vpn] mpls l2vpn
[PE1-l2vpn] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE1] vlan 2
[PE1-vlan2] port GigabitEthernet 2/0/2
[PE1-vlan2] quit
```

Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

Configure OSPF on PE 1 for establishing LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

3. Configure a VC ID for the CE that connects to Customer A site 1:

Establish a remote session to PE 2.

```
[PE1] mpls ldp remote-peer 1
```

```
[PE1-mpls-ldp-remote-1] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-1] quit
```

Create a Martini VC on the interface that connects to CE 1. Specify the peer PE IP address as 3.3.3.9 and VC ID as 101.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] mpls l2vc 3.3.3.9 101
[PE1-Vlan-interface11] quit
```

Configuring P

1. Configure an LSR ID, and enable MPLS globally.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] mpls lsr-id 2.2.2.9
[P] mpls
```

2. Allow all routing entries to trigger the establishment of LSPs.

```
[P-mpls] lsp-trigger all
[P-mpls] quit
```

3. Enable LDP globally.

```
[P] mpls ldp
[P-mpls-ldp] quit
```

4. Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[P] vlan2
[P-vlan2] port GigabitEthernet2/0/2
[P-vlan2] quit
```

5. Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
```

6. Create VLAN 3, and assign GigabitEthernet 2/0/1 to the VLAN.

```
[P] vlan3
[P-vlan3] port GigabitEthernet2/0/1
[P-vlan3] quit
```

7. Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

8. Configure OSPF on P for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 1.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configuring PE 2

1. Create VLAN 11, assign GigabitEthernet 2/0/4 to VLAN 11, and create VLAN-interface 11.

```
[PE2] vlan 11
[PE2-vlan11] port GigabitEthernet 2/0/4
[PE2-vlan11] quit
[PE2] interface Vlan-interface 11
[PE2-Vlan-interface11] quit
```

2. Configure LDP to generate the outer label:

Configure an LSR ID, and enable MPLS globally.

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
```

Allow all routing entries to trigger the establishment of LSPs.

```
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
```

Enable MPLS L2VPN and LDP globally.

```
[PE2] l2vpn
[PE2-l2vpn] mpls l2vpn
[PE2-l2vpn] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

Create VLAN 3, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE2] vlan 3
[PE2-vlan3] port GigabitEthernet 2/0/2
[PE2-vlan3] quit
```

Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.2 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

3. Configure a VC ID for the CE that connects to Customer A site 1:

Establish a remote session to PE 2.

```
[PE2] mpls ldp remote-peer 2
```

```
[PE2-mpls-ldp-remote-2] remote-ip 1.1.1.9
[PE2-mpls-ldp-remote-2] quit
```

Create a Martini VC on the interface that connects to CE 3. Specify the peer PE IP address as 1.1.1.9 and VC ID as 101.

```
[PE2] interface vlan-interface 11
[PE2-Vlan-interface11] mpls l2vc 1.1.1.9 101
[PE2-Vlan-interface11] quit
```

Providing VPN services for Customer B

On CE 2 and CE 4, assign the interfaces that connect to the PEs to the VLAN to which Customer B belongs. For more information about the configuration, see "Configuring CEs."

When a new CE connects to a PE, perform the following configurations:

- Configure a Martini VC on the CE's interface that connects to the PE.
- Specify the PE's IP address and the VC ID.

1. Configure PE1:

   # Create VLAN 10, assign GigabitEthernet 2/0/1 to VLAN 10, and create VLAN-interface 10.

   ```
   [PE1] vlan 10
   [PE1-vlan10] port GigabitEthernet 2/0/1
   [PE1-vlan10] quit
   [PE1] interface Vlan-interface 10
   ```

   # Create a Martini VC on the interface that connects to CE 2. Specify the peer PE IP address as 3.3.3.9 and VC ID as 201.

   ```
   [PE1-Vlan-interface10] mpls l2vc 3.3.3.9 201
   [PE1-Vlan-interface10] quit
   ```

2. Configure PE2:

   # Create VLAN 10, assign GigabitEthernet 2/0/1 to VLAN 10, and create VLAN-interface 10.

   ```
   [PE2] vlan 10
   [PE2-vlan10] port GigabitEthernet 2/0/1
   [PE2-vlan10] quit
   [PE2] interface Vlan-interface 10
   ```

   # Create a Martini VC on the interface that connects to CE 4. Specify the peer PE IP address as 1.1.1.9 and VC ID as 201.

   ```
   [PE2-Vlan-interface10] mpls l2vc 1.1.1.9 201
   [PE2-Vlan-interface10] quit
   ```

Verifying the configuration

- Verify Layer 2 VPN information for Customer A:

  # Display VC information on PE 1. The output shows that a VC has been established.

  ```
  [PE1] display mpls l2vc
  Total ldp vc : 1     1 up       0 down

  Transport  Client     Service       VC      Local      Remote     Tunnel
  VC ID      Intf       ID            State   VC Label   VC Label   Policy
  101        Vlan11     --            up      8193       8192       default
  ```

  # Display VC information on PE 2. The output shows that a VC has been established.

```
[PE2] display mpls l2vc
Total ldp vc : 1     1 up       0 down
Transport  Client      Service      VC      Local      Remote     Tunnel
VC ID      Intf        ID           State   VC Label   VC Label   Policy
101        Vlan11      --           up      8192       8193       default
```

The output shows the following:

- PE 1 has assigned the inner label 8193 to the VC whose VC ID is 101.
- PE 2 has assigned the inner label 8192 to the same VC.
- The PEs have advertised the inner labels to each other.

Verify that the host and the server in different sites of Customer A can reach each other. If they can, you can conclude that the MPLS L2VPN has been established.

- Verify Layer 2 VPN information for Customer B:

Display VC information on PE 1. The output shows that a new VC has been established.

```
[PE1] display mpls l2vc
Total ldp vc : 2     2 up       0 down

Transport  Client     Service       VC      Local      Remote     Tunnel
VC ID      Intf       ID            State   VC Label   VC Label   Policy
101        Vlan11     --            up      8193       8192       default
201        Vlan10     --            up      8194       8193       default
```

Display VC information on PE 2. The output shows that a new VC has been established.

```
[PE2] display mpls l2vc
Total ldp vc : 2     2 up       0 down
Transport  Client     Service       VC      Local      Remote     Tunnel
VC ID      Intf       ID            State   VC Label   VC Label   Policy
101        Vlan11     --            up      8192       8193       default
201        Vlan11     --            up      8193       8194       default
```

Configuration files

- CE 1 and CE 2:

```
#
 vlan 100
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk permit vlan 100
```

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 10 to 11
#
mpls
```

```
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.9
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface10
 mpls l2vc 3.3.3.9 201
#
interface Vlan-interface11
 mpls l2vc 3.3.3.9 101
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet2/0/4
 port link-mode bridge
 port access vlan 11
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 10 to 11
```

```
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 2
 remote-ip 1.1.1.9
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface10
 mpls l2vc 1.1.1.9 201
#
interface Vlan-interface11
 mpls l2vc 1.1.1.9 101
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet2/0/4
 port link-mode bridge
 port access vlan 11
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
```

- P:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 3
```

```
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2

#
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
  network 3.3.3.9 0.0.0.0
#
```

Example: Configuring service instance-based Martini MPLS L2VPN

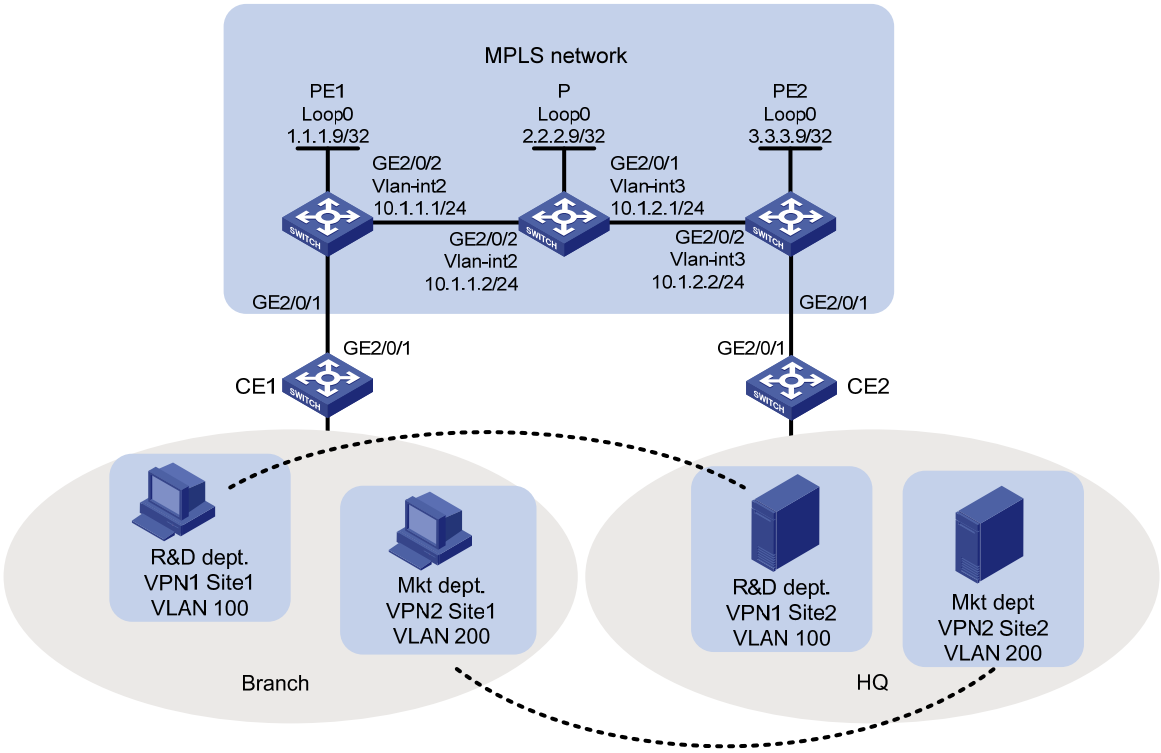
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 135, configure service instance-based Martini MPLS L2VPN so the R&D department and the Marketing department use different VPN connections to achieve data isolation.

Figure 135 Network diagram



Configuration procedures

Configuring CEs

On each CE, configure the interface that connects to the PE to permit tagged packets from the customer VLAN. This example uses CE 1.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] vlan 200
[CE1-vlan200] quit
[CE1] interface GigabitEthernet 2/0/1
[CE1-GigabitEthernet2/0/1] port link-type trunk
[CE1-GigabitEthernet2/0/1] port trunk permit vlan 100 200
```

Configuring PE 1

1. Configure LDP to generate the outer label:

   # Configure an LSR ID, and enable MPLS globally.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
```

   # Allow all routing entries to trigger the establishment of LSPs.

```
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
```

   # Enable MPLS L2VPN and LDP globally.

```
[PE1] l2vpn
[PE1-l2vpn] mpls l2vpn
[PE1-l2vpn] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

   # Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE1] vlan 2
[PE1-vlan2] port GigabitEthernet 2/0/2
[PE1-vlan2] quit
```

   # Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

   # Configure OSPF on PE 1 for establishing LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

2. Configure a service instance for each department, and bind the service instance with a VC:

   # Establish a remote session to PE 2.

```
[PE1] mpls ldp remote-peer 1
[PE1-mpls-ldp-remote-1] remote-ip  3.3.3.9
[PE1-mpls-ldp-remote-1] quit
```

   # Configure GigabitEthernet 2/0/1 as a trunk port. Configure the port to permit tagged packets from VLAN 100 and VLAN 200.

```
[PE1] interface GigabitEthernet 2/0/1
[PE1-GigabitEthernet2/0/1] port link-type trunk
[PE1-GigabitEthernet2/0/1] port trunk permit vlan 100 200
```

Create service instance 100 on GigabitEthernet 2/0/1. Configure a packet matching rule in the service instance to match traffic that carries outer VLAN ID 100.

```
[PE1-GigabitEthernet2/0/1] service-instance 100
[PE1-GigabitEthernet2/0/1-srv100] encapsulation s-vid 100
```

For service instance 100, create a Martini VC, and specify the remote peer IP address as 3.3.3.9 and the PW ID of the VC as 100.

```
[PE1-GigabitEthernet2/0/1-srv100] xconnect peer 3.3.3.9 pw-id 100
```

Create service instance 200 on GigabitEthernet 2/0/1. Configure a packet matching rule in the service instance to match traffic that carries outer VLAN ID 200.

```
[PE1-GigabitEthernet2/0/1] service-instance 200
[PE1-GigabitEthernet2/0/1-srv200] encapsulation s-vid 200
```

For service instance 200, create a Martini VC, and specify the remote peer IP address as 3.3.3.9 and the PW ID of the VC as 200.

```
[PE1-GigabitEthernet2/0/1-srv200] xconnect peer 3.3.3.9 pw-id 200
```

Configuring P

1. Configure an LSR ID, and enable MPLS globally.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] mpls lsr-id 2.2.2.9
[P] mpls
```

2. Allow all routing entries to trigger the establishment of LSPs.

```
[P-mpls] lsp-trigger all
[P-mpls] quit
```

3. Enable LDP globally.

```
[P] mpls ldp
[P-mpls-ldp] quit
```

4. Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[P] vlan2
[P-vlan2] port GigabitEthernet2/0/2
[P-vlan2] quit
```

5. Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
```

6. Create VLAN 3, and assign GigabitEthernet 2/0/1 to the VLAN.

```
[P] vlan3
[P-vlan3] port GigabitEthernet2/0/1
[P-vlan3] quit
```

7. Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] mpls
```

```
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

8. Configure OSPF on P for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 1.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configuring PE 2

1. Configure LDP to generate the outer label:

   # Configure an LSR ID, and enable MPLS globally.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
```

   # Allow all routing entries to trigger the establishment of LSPs.

```
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
```

   # Enable MPLS L2VPN and LDP globally.

```
[PE2] l2vpn
[PE2-l2vpn] mpls l2vpn
[PE2-l2vpn] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

   # Create VLAN 3, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE2] vlan 3
[PE2-vlan3] port GigabitEthernet 2/0/2
[PE2-vlan3] quit
```

   # Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

   # Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

2. Configure a service instance for each department and bind the service instance with a VC:

Establish a remote session to PE 1.

```
[PE2] mpls ldp remote-peer 1
[PE2-mpls-ldp-remote-1] remote-ip  1.1.1.9
[PE2-mpls-ldp-remote-1] quit
```

Configure GigabitEthernet 2/0/1 as a trunk port. Configure the port to permit tagged packets from VLAN 100 and VLAN 200.

```
[PE2] interface GigabitEthernet 2/0/1
[PE2-GigabitEthernet2/0/1] port link-type trunk
[PE2-GigabitEthernet2/0/1] port trunk permit vlan 100 200
```

Create service instance 100 on GigabitEthernet 2/0/1. Configure a packet matching rule in the service instance to match traffic that carries outer VLAN ID 100.

```
[PE2-GigabitEthernet2/0/1] service-instance 100
[PE2-GigabitEthernet2/0/1-srv100] encapsulation s-vid 100
```

For service instance 100, create a Martini VC, and specify the remote peer IP address as 1.1.1.9 and the PW ID of the VC as 100.

```
[PE2-GigabitEthernet2/0/1-srv100] xconnect peer 1.1.1.9 pw-id 100
```

Create service instance 200 on GigabitEthernet 2/0/1. Configure a packet matching rule in the service instance to match traffic that carries outer VLAN ID 200.

```
[PE2-GigabitEthernet2/0/1] service-instance 200
[PE2-GigabitEthernet2/0/1-srv200] encapsulation s-vid 200
```

For service instance 200, create a Martini VC, and specify the remote peer IP address as 1.1.1.9 and the PW ID of the VC as 200.

```
[PE2-GigabitEthernet2/0/1-srv200] xconnect peer 1.1.1.9 pw-id 200
```

Verifying the configuration

Display VC information on PE 1. The output shows that two VCs have been established.

```
[PE1] display mpls l2vc

Total ldp vc : 2     2 up       0 down

Transport   Client     Service      VC      Local      Remote
VC ID       Intf       ID           State   VC Label   VC Label
100         GE2/0/1    100          up      8193       8192
200         GE2/0/1    200          up      8194       8193
```

Display VC information on PE 2. The output shows that two VCs have been established.

```
[PE2] display mpls l2vc

Total ldp vc : 2     2 up       0 down

Transport   Client     Service      VC      Local      Remote
VC ID       Intf       ID           State   VC Label   VC Label
100         GE2/0/1    100          up      8192       8193
200         GE2/0/1    200          up      8193       8194
```

The output shows the following:

- PE 1 has assigned the inner label 8193 to the VC that is bound to service instance 100.

- PE 2 has assigned the inner label 8192 to the VC that is bound to service instance 100.
- PE 1 has assigned the inner label 8194 to the VC that is bound to service instance 200.
- PE 2 has assigned the inner label 8193 to the VC that is bound to service instance 200.

The PEs have advertised the inner labels to each other.

Verify that the host and the server in different sites of Customer A can reach other. If they can, you can conclude that the MPLS L2VPN has been established.

Configuration files

- CE 1 and CE 2:

```
#
 vlan 100
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk permit vlan 100
```

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.9
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
 service-instance 100
  encapsulation s-vid 100
```

```
  xconnect peer 3.3.3.9 pw-id 100
 service-instance 200
  encapsulation s-vid 200
  xconnect peer 3.3.3.9 pw-id 200
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.9
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
 service-instance 100
  encapsulation s-vid 100
  xconnect peer 1.1.1.9 pw-id 100
 service-instance 200
  encapsulation s-vid 200
  xconnect peer 1.1.1.9 pw-id 200
#
ospf 1
 area 0.0.0.0
```

```
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
```

- P:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 3
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2

#
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
  network 3.3.3.9 0.0.0.0
#
```

Example: Configuring Kompella MPLS L2VPN

Applicable product matrix

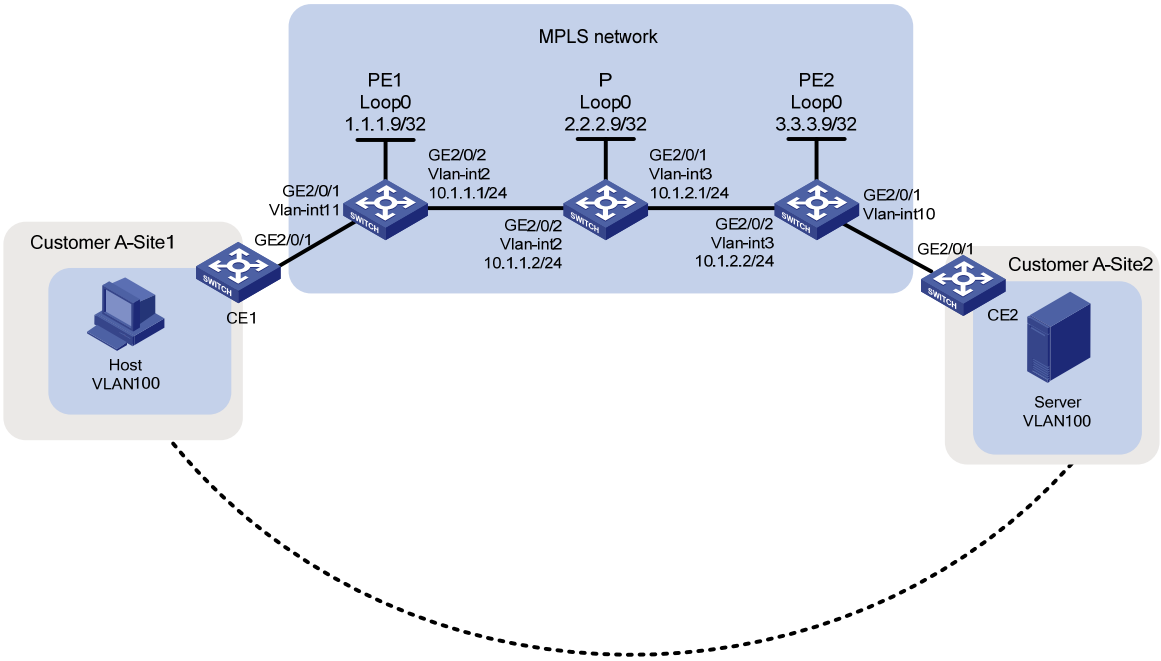
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 136, a customer has two VPN sites and will add 12 sites in the future.

Configure Kompella MPLS L2VPN so that new sites can be added with simple configurations.

Figure 136 Network diagram



Configuration restrictions and guidelines

When you configure Kompella MPLS L2VPN, follow these restrictions and guidelines:

- On each PE, create an L2VPN instance for each CE connected to the PE.
- On each PE, the VC encapsulation type specified for a L2VPN must be the same as the encapsulation type of the interface that connects to the CE.

Configuration procedures

Configuring CEs

On each CE, configure the interface that connects to the PE to permit tagged packets from the customer VLAN. This example uses CE 1.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface GigabitEthernet 2/0/1
[CE1-GigabitEthernet2/0/1] port link-type trunk
[CE1-GigabitEthernet2/0/1] port trunk permit vlan 100
```

Establishing LDP LSPs

1. Configure PE 1:

   # Allow all routing entries to trigger the establishment of LSPs.

   ```
   [PE1] mpls
   [PE1-mpls] lsp-trigger all
   [PE1-mpls] quit
   ```

   # Enable LDP globally.

   ```
   [PE1] mpls ldp
   [PE1-mpls-ldp] quit
   ```

   # Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

   ```
   [PE1] vlan 2
   [PE1-vlan2] port GigabitEthernet 2/0/2
   [PE1-vlan2] quit
   ```

   # Configure VLAN-interface 2, and enable MPLS and LDP on it.

   ```
   [PE1] interface vlan-interface 2
   [PE1-Vlan-interface2] ip address 10.1.1.1 24
   [PE1-Vlan-interface2] mpls
   [PE1-Vlan-interface2] mpls ldp
   [PE1-Vlan-interface2] quit
   ```

   # Configure OSPF on PE 1 for establishing LSPs.

   ```
   [PE1] ospf
   [PE1-ospf-1] area 0
   [PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
   [PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
   [PE1-ospf-1-area-0.0.0.0] quit
   [PE1-ospf-1] quit
   ```

2. Configure P:

   # Configure an LSR ID, and enable MPLS globally.

   ```
   <P> system-view
   [P] interface loopback 0
   [P-LoopBack0] ip address 2.2.2.9 32
   [P-LoopBack0] quit
   [P] mpls lsr-id 2.2.2.9
   [P] mpls
   ```

Allow all routing entries to trigger the establishment of LSPs.

```
[P-mpls] lsp-trigger all
[P-mpls] quit
```

Enable LDP globally.

```
[P] mpls ldp
[P-mpls-ldp] quit
```

Create VLAN 2, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[P] vlan2
[P-vlan2] port GigabitEthernet2/0/2
[P-vlan2] quit
```

Configure VLAN-interface 2, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
```

Create VLAN 3, and assign GigabitEthernet 2/0/1 to the VLAN.

```
[P] vlan3
[P-vlan3] port GigabitEthernet2/0/1
[P-vlan3] quit
```

Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

Configure OSPF on P for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 1.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

3. Configure PE 2:

Configure an LSR ID, and enable MPLS globally.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
```

Allow all routing entries to trigger the establishment of LSPs.

```
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
```

Enable MPLS L2VPN and LDP globally.

```
[PE2] mpls l2vpn
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

Create VLAN 3, and assign GigabitEthernet 2/0/2 to the VLAN.

```
[PE2] vlan 3
[PE2-vlan3] port GigabitEthernet 2/0/2
[PE2-vlan3] quit
```

Configure VLAN-interface 3, and enable MPLS and LDP on it.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.2 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configuring BGP connections between PE 1 and PE 2 and connections between CE 1 and CE 2

1. Configure BGP connections between PE 1 and PE 2:

On PE 1, enable BGP.

```
[PE1] bgp 100
```

Configure peer 3.3.3.9: specify the local AS number as 100, and specify loopback 0 as the source interface for advertising routing updates to PE 2.

```
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
```

Enable the peer for the BGP-L2VPN address family. Enable route target-based filtering for incoming VPNv4 routes.

```
[PE1-bgp] l2vpn-family
[PE1-bgp-af-l2vpn] policy vpn-target
[PE1-bgp-af-l2vpn] peer 3.3.3.9 enable
[PE1-bgp-af-l2vpn] quit
[PE1-bgp] quit
```

On PE 2, create VLAN-interface 10.

```
[PE2] vlan 10
[PE2-vlan10] quit
[PE2] interface vlan-interface 10
[PE2-Vlan-interface10] quit
```

Configure GigabitEthernet 2/0/1 as a trunk port, and assign the port to VLAN 10.

```
[PE2] interface GigabitEthernet 2/0/1
[PE2-GigabitEthernet2/0/1] port link-type trunk
[PE2-GigabitEthernet2/0/1] port trunk permit vlan 10
[PE2-GigabitEthernet2/0/1] quit
```

On PE 2, enable BGP.

```
[PE2] bgp 100
```

Configure peer 1.1.1.9: specify the local AS number as 100, and specify loopback 0 as the source interface for advertising routing updates to PE 1.

```
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
```

Enable the peer for the BGP-L2VPN address family. Enable route target-based filtering for incoming VPNv4 routes.

```
[PE2-bgp] l2vpn-family
[PE2-bgp-af-l2vpn] policy vpn-target
[PE2-bgp-af-l2vpn] peer 1.1.1.9 enable
[PE2-bgp-af-l2vpn] quit
[PE2-bgp] quit
```

Execute the **display bgp l2vpn peer** command to verify that a peer relationship in Established state has been established between PE 1 and PE 2. This example uses PE 1.

```
[PE1] display bgp l2vpn peer
BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1
  Peer         AS   MsgRcvd   MsgSent  OutQ PrefRcv Up/Down  State
  3.3.3.9      100        2        5     0       0  00:01:07 Established
```

2. Configure connections between CE 1 and CE 2:

On PE 2, create a Kompella MPLS L2VPN with the VPN name of **vpn_a** and the VC encapsulation type of **VLAN**.

```
[PE2] mpls l2vpn vpn_a encapsulation vlan
```

On PE 2, configure the same RD and route target for the VPN as those configured on PE 1.

```
[PE2-mpls-l2vpn-vpn_a] route-distinguisher 100:1
[PE2-mpls-l2vpn-vpn_a] vpn-target 100:1
```

On PE 2, set the CE ID of CE 2 to 2, and set the maximum number of CEs in the VPN to 14.

```
[PE2-mpls-l2vpn-vpn_a] ce ce2 id 2 range 14
```

On PE 2, create a Kompella connection between CE 2 and CE 1.

```
[PE2-mpls-l2vpn-ce-vpn_a-ce2] connection ce-offset 1 interface Vlan-interface10
```

On PE 1, create a Kompella connection between CE 1 and CE 2.

```
[PE1] mpls l2vpn vpn_a encapsulation vlan
[PE1-mpls-l2vpn-vpn_a] ce ce1
[PE1-mpls-l2vpn-ce-vpn_a-ce1] connection ce-offset 2 interface vlan-interface 11
[PE1-mpls-l2vpn-ce-vpn_a-ce1] quit
```

Verifying the configuration

Execute the **display mpls l2vpn connection** command to verify that a remote L2VPN connection in up state has been established. This example uses PE 1.

```
[PE1] display mpls l2vpn connection
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
VPN name: vpn_a,
1 total connections,
```

```
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
  CE name: ce1, id: 1,
  Rid type status peer-id         route-distinguisher   intf
  2   rmt  up     3.3.3.9         100:1                Vlan11
```

Ping the host from the server or ping the server from the host. If the ping operation succeeds, you can conclude that the VPN has been established.

Configuration files

- CE 1 and CE 2:

```
#
 vlan 100
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk permit vlan 100
```

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 11
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface11
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2
```

```
#
bgp 100
 undo synchronization
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 #
 l2vpn-family
  peer 3.3.3.9 enable
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
mpls l2vpn vpn_a encapsulation vlan
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
 ce ce1 id 1 range 14 default-offset 0
  connection ce-offset 2 interface Vlan-interface11
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 11
#
mpls
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface10
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 3
```

```
#
bgp 100
 undo synchronization
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 #
 l2vpn-family
  peer 1.1.1.9 enable
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
mpls l2vpn vpn_a encapsulation vlan
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
 ce ce2 id 2 range 14 default-offset 0
  connection ce-offset 1 interface Vlan-interface10
```

- P:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 3
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
```

```
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2

#
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
  network 3.3.3.9 0.0.0.0
#
```

Multicast VLAN configuration examples

This document provides examples for configuring multicast VLANs to reduce the traffic load on Layer 3 devices.

Multicast VLANs include sub-VLAN-based multicast VLANs and port-based multicast VLANs.

- In a sub-VLAN-based multicast VLAN, IGMP snooping manages router ports in the multicast VLAN and user ports in each sub-VLAN. It is applicable to all networking environments.
- In a port-based multicast VLAN, IGMP snooping manages both router ports and user ports in the multicast VLAN. Port-based multicast VLAN is typically deployed on devices that are directly connected to receivers. Port-based multicast VLAN is easier to implement than sub-VLAN-based multicast VLAN.

General configuration restrictions and guidelines

When you configure multicast VLANs, follow these restrictions and guidelines:

- Do not configure multicast VLAN on a device with multicast routing enabled.
- The port-based multicast VLAN takes precedence over the sub-VLAN-based multicast VLAN if they are both configured on a device.

Example: Configuring a sub-VLAN-based multicast VLAN

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

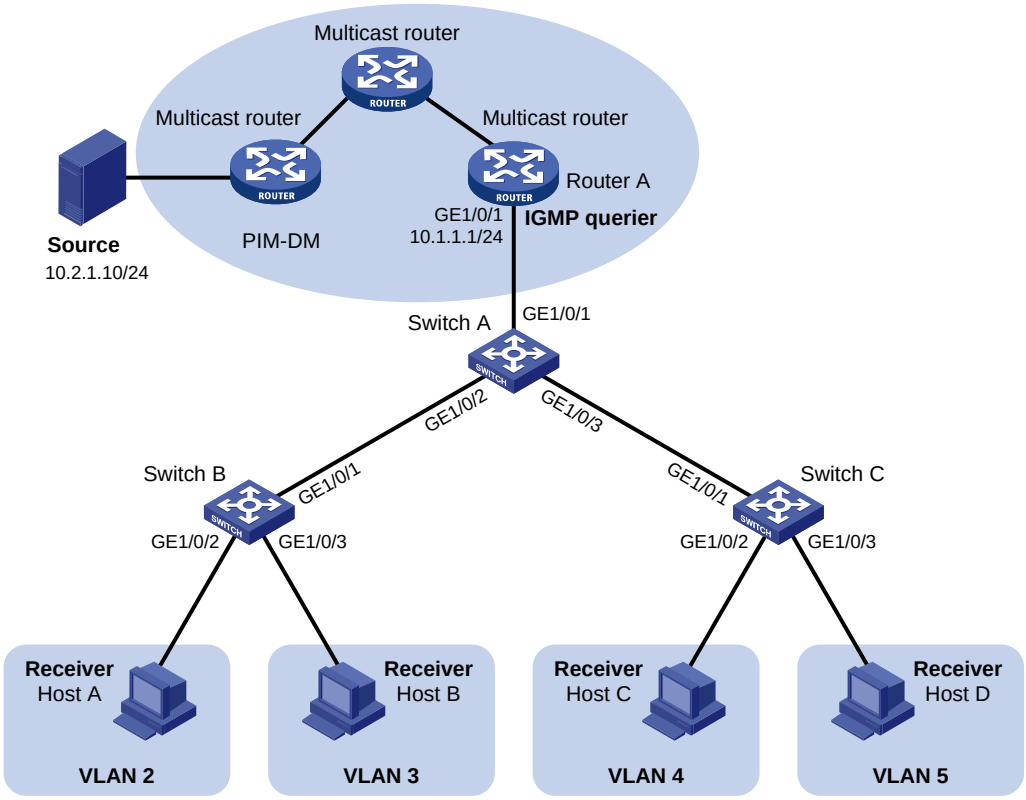
Network requirements

As shown in Figure 137:

- The Layer 2 user network is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- Each user VLAN has a receiver that belongs to the same multicast group.

To save bandwidth and reduce the burden on Layer 3 multicast routers, configure a sub-VLAN-based multicast VLAN on Switch A. In this scenario, Layer 3 multicast routers only need to forward multicast data to the multicast VLAN. Receiver hosts in different user VLANs can receive the data.

Figure 137 Network diagram



Configuration restrictions and guidelines

When you configure a sub-VLAN-based multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as a multicast VLAN must exist.
- The VLAN to be configured as a sub-VLAN must exist and cannot be a multicast VLAN or a sub-VLAN of any other multicast VLANs.
- After you enable IGMP snooping for the multicast VLAN, the sub-VLANs are automatically enabled with IGMP snooping.

Configuration procedures

Configuring Switch A

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 2 through VLAN 5. Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLAN 2 and VLAN 3.

```
[SwitchA] vlan 2 to 5
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 2 3
```

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

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 4 and VLAN 5.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4 5
[SwitchA-GigabitEthernet1/0/3] quit
```

Create VLAN 1024, and assign GigabitEthernet 1/0/1 to this VLAN.

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1
```

Enable IGMP snooping for VLAN 1024.

```
[SwitchA-vlan1024] igmp-snooping enable
[SwitchA-vlan1024] quit
```

Configure VLAN 1024 as the multicast VLAN.

```
[SwitchA] multicast-vlan 1024
```

Configure VLAN 2 through VLAN 5 as the sub-VLANs.

```
[SwitchA-mvlan-1024] subvlan 2 to 5
```

Configuring Switch B

Enable IGMP snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 2, and assign GigabitEthernet 1/0/2 to this VLAN.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
```

Enable IGMP snooping for VLAN 2.

```
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
```

Create VLAN 3, and assign GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
```

Enable IGMP snooping for VLAN 3.

```
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
```

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

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2 3
```

Configuring Switch C

Configure Switch C in the same way Switch B is configured. (Details not shown.)

Verifying the configuration

1. Send IGMP reports from the receiver hosts in the user VLANs to the multicast group 224.1.1.1.

2. Verify that Switch A can receive the reports and that it forwards the reports to Router A.

Display information about the multicast VLAN on Switch A.

```
[SwitchA] display multicast-vlan
Total 1 multicast-vlan(s)

 Multicast vlan 1024
   subvlan list:
    vlan 2-5
   port list:
    no port
```

Display IGMP snooping group information on Switch A.

```
[SwitchA] display igmp-snooping group
  Total 5 IP Group(s).
  Total 5 IP Source(s).
  Total 5 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 1 port.
            GE1/0/2                  (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            GE1/0/2

  Vlan(id):3.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 1 port.
            GE1/0/2                  (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            GE1/0/2
```

```
 Vlan(id):4.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 1 port.
            GE1/0/3                  (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            GE1/0/3

 Vlan(id):5.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 1 port.
            GE1/0/3                  (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            GE1/0/3

 Vlan(id):1024.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/1                  (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 0 port.
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 0 port.
```

The output shows the following:

- IGMP snooping in the multicast VLAN (VLAN 1024) maintains the router ports.
- IGMP snooping in the sub-VLANs (VLAN 2 through VLAN 5) maintains the member ports.

Configuration files

```
#
 igmp-snooping
#
vlan 2 to 5
#
vlan 1024
 igmp-snooping enable
#
multicast-vlan 1024
 subvlan 2 to 5
#
interface GigabitEthernet1/0/1
 port access vlan 1024
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 3
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 4 to 5
#
```

Example: Configuring a port-based multicast VLAN

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

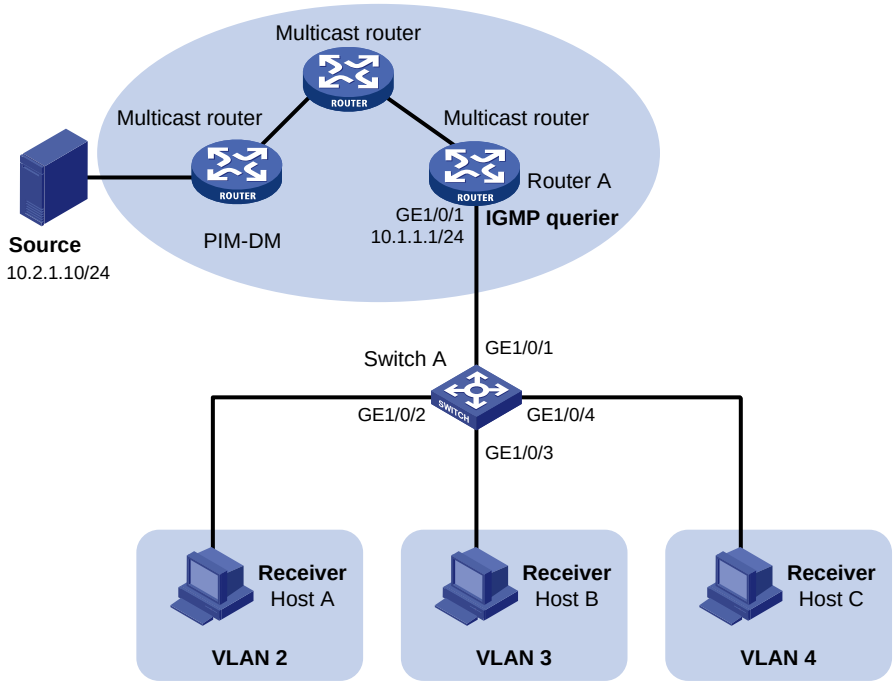
Network requirements

As shown in Figure 138:

- The Layer 2 user network is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- Each user VLAN has a receiver that belongs to the same multicast group, and the receiver hosts are directly connected to Switch A.

To save bandwidth and reduce the burden on Layer 3 multicast routers, configure a port-based multicast VLAN on Switch A. In this scenario, Layer 3 multicast routers only need to send multicast data to the multicast VLAN. Receiver hosts in different user VLANs can receive the data.

Figure 138 Network diagram



Configuration restrictions and guidelines

When you configure a port-based multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as the multicast VLAN must exist.
- A port can belong to only one multicast VLAN.
- You must enable IGMP snooping for the multicast VLAN and the user VLANs.
- The user ports must be hybrid ports. You must assign user ports to the multicast VLAN and user VLANs as untagged VLAN members.

Configuration procedures

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 1024, and assign GigabitEthernet 1/0/1 to this VLAN.

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1
```

Enable IGMP snooping for VLAN 1024.

```
[SwitchA-vlan1024] igmp-snooping enable
[SwitchA-vlan1024] quit
```

Create VLAN 2, and enable IGMP snooping for this VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
```

```
[SwitchA-vlan2] quit
```

Configure VLAN 3 and VLAN 4 in the same way. (Details not shown.)

Configure GigabitEthernet 1/0/2 as a hybrid port, and configure VLAN 2 as the PVID.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
```

Assign GigabitEthernet 1/0/2 to VLAN 2 and VLAN 1024 as an untagged VLAN member.

```
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 1024 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a hybrid port, and configure VLAN 3 as the PVID.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type hybrid
[SwitchA-GigabitEthernet1/0/3] port hybrid pvid vlan 3
```

Assign GigabitEthernet 1/0/3 to VLAN 3 and VLAN 1024 as an untagged VLAN member.

```
[SwitchA-GigabitEthernet1/0/3] port hybrid vlan 3 1024 untagged
[SwitchA-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/4 as a hybrid port, and configure VLAN 4 as the PVID.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type hybrid
[SwitchA-GigabitEthernet1/0/4] port hybrid pvid vlan 4
```

Assign GigabitEthernet 1/0/4 to VLAN 4 and VLAN 1024 as an untagged VLAN member.

```
[SwitchA-GigabitEthernet1/0/4] port hybrid vlan 4 1024 untagged
[SwitchA-GigabitEthernet1/0/4] quit
```

Configure VLAN 1024 as the multicast VLAN.

```
[SwitchA] multicast-vlan 1024
```

Assign GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 to VLAN 1024.

```
[SwitchA-mvlan-1024] port gigabitethernet 1/0/2 to gigabitethernet 1/0/4
[SwitchA-mvlan-1024] quit
```

Verifying the configuration

1. Send IGMP reports from the hosts in the user VLANs to join the multicast group address 224.1.1.1. Verify that Switch A can receive the reports and that it forwards them to Router A.
2. Verify that Switch A can receive the reports and that it forwards them to Router A.

   # Display information about the multicast VLAN on Switch A.

   ```
   [SwitchA] display multicast-vlan
    Total 1 multicast-vlan(s)

   Multicast vlan 1024
      subvlan list:
       no subvlan
      port list:
       GE1/0/2                 GE1/0/3                 GE1/0/4
   ```

   # Display IGMP snooping group information on Switch A.

```
[SwitchA] display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):1024.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/1                 (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 3 port.
            GE1/0/2                 (D)
            GE1/0/3                 (D)
            GE1/0/4                 (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 3 port.
            GE1/0/2
            GE1/0/3
            GE1/0/4
```

The output shows that IGMP snooping in the multicast VLAN (VLAN 1024) maintains the router port and the member ports.

Configuration files

```
#
igmp-snooping
#
vlan 2
 igmp-snooping enable
#
vlan 3
 igmp-snooping enable
#
vlan 4
 igmp-snooping enable
#
vlan 1024
 igmp-snooping enable
#
multicast-vlan 1024
#
```

```
interface GigabitEthernet1/0/1
 port access vlan 1024
#
interface GigabitEthernet1/0/2
 port link-type hybrid
 port hybrid vlan 1 to 2 1024 untagged
 port hybrid pvid vlan 2
 port multicast-vlan 1024
#
interface GigabitEthernet1/0/3
 port link-type hybrid
 port hybrid vlan 1 3 1024 untagged
 port hybrid pvid vlan 3
 port multicast-vlan 1024
#
interface GigabitEthernet1/0/4
 port link-type hybrid
 port hybrid vlan 1 4 1024 untagged
 port hybrid pvid vlan 4
 port multicast-vlan 1024
#
```

NetStream configuration examples

This chapter provides an IPv4 NetStream configuration example and an IPv6 NetStream configuration example.

Example: Configuring IPv4 NetStream

Applicable product matrix

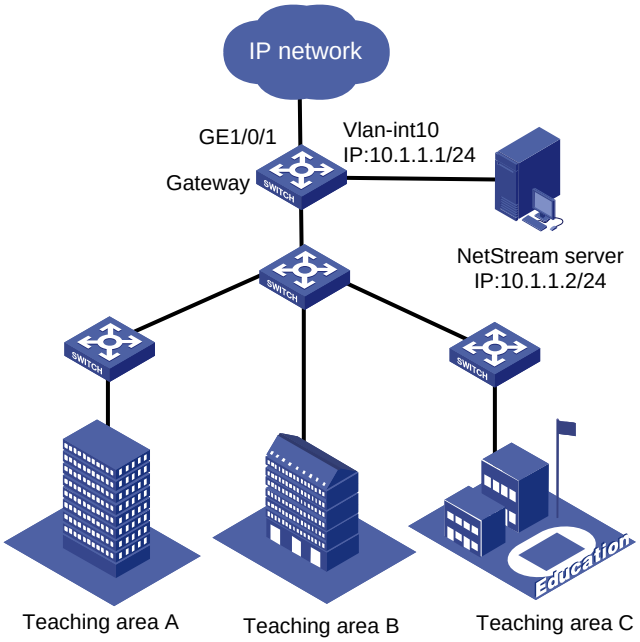
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 139, a school is divided into three teaching areas, each with the same bandwidth.

With the application of VoIP, P2P, and IPTV, configure IPv4 NetStream on Gateway so the administrator can obtain information about bandwidth utilization for network planning and traffic monitoring.

Figure 139 Network diagram



Configuration restrictions and guidelines

When you configure IPv4 NetStream, follow these restrictions and guidelines:

- This section focuses on the description and configuration of Gateway that acts as an NDE.
- The destination UDP port number configured on Gateway must be the same as the UDP port number of the NetStream server.
- Configurations in NetStream aggregation view only apply to aggregation data export. Configurations in system view apply to NetStream traditional data export.
- To reduce the bandwidth consumption of the NetStream data, merge the flows into one aggregation flow if each aggregation criterion is of the same value.

Configuration procedures

Enable NetStream for incoming and outgoing traffic on GigabitEthernet 1/0/1.

```
<Gateway> system-view
[Gateway] interface GigabitEthernet 1/0/1
[Gateway-GigabitEthernet1/0/1] ip netstream inbound
[Gateway-GigabitEthernet1/0/1] ip netstream outbound
[Gateway-GigabitEthernet1/0/1] quit
```

Configure VLAN-interface 10 as the source interface for NetStream data export.

```
[Gateway] vlan 10
[Gateway-vlan10] quit
[Gateway] interface vlan-interface 10
[Gateway-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
[Gateway-Vlan-interface10] quit
[Gateway] ip netstream export source interface Vlan-interface 10
```

Configure the destination address for NetStream traditional data export as 10.1.1.2 with port 5000.

```
[Gateway] ip netstream export host 10.1.1.2 5000
```

Set the aggregation mode as protocol-port. Configure the destination address for NetStream aggregation data export as 10.1.1.2 with port 5000.

```
[Gateway] ip netstream aggregation protocol-port
[Gateway-ns-aggregation-protport] enable
[Gateway-ns-aggregation-protport] ip netstream export host 10.1.1.2 5000
[Gateway-ns-aggregation-protport] quit
```

Set the aggregation mode as tos-protocol-port. Configure the destination address for NetStream aggregation data export as 10.1.1.2 with port 5000.

```
[Gateway] ip netstream aggregation tos-protocol-port
[Gateway-ns-aggregation-tosprotport] enable
[Gateway-ns-aggregation-tosprotport] ip netstream export host 10.1.1.2 5000
[Gateway-ns-aggregation-tosprotport] quit
```

Verifying the configuration

Display the statistics of NetStream data export.

```
[Gateway] display ip netstream export
IP export information:
  Stream source interface                    : Vlan-interface10
  Stream destination VPN-instance            :
  Stream destination IP (UDP)                : 10.1.1.2 (5000)
```

```
  Version 5 exported stream number               : 8
  Version 5 exported UDP datagram number (failed): 8 (0)
  Version 9 exported stream number               : 0
  Version 9 exported UDP datagram number (failed): 0 (0)

L2 export information:
  Stream source interface                        : Vlan-interface10
  Stream destination VPN-instance                :
  Stream destination IP (UDP)                    : 10.1.1.2 (5000)
  Version 9 exported stream number               : 0
  Version 9 exported UDP datagram number (failed): 0 (0)

protocol-port aggregation export information:
  Stream source interface                        : Vlan-interface10
  Stream destination VPN-instance                :
  Stream destination IP (UDP)                    : 10.1.1.2 (5000)
  Version 8 exported stream number               : 3
  Version 8 exported UDP datagram number (failed): 3 (0)
  Version 9 exported stream number               : 0
  Version 9 exported UDP datagram number (failed): 0 (0)

tos-protocol-port aggregation export information:
  Stream source interface                        : Vlan-interface10
  Stream destination VPN-instance                :
  Stream destination IP (UDP)                    : 10.1.1.2 (5000)
  Version 8 exported stream number               : 6
  Version 8 exported UDP datagram number (failed): 6 (0)
  Version 9 exported stream number               : 0
  Version 9 exported UDP datagram number (failed): 0 (0)
```

Configuration files

```
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip netstream inbound
 ip netstream outbound
#
 ip netstream export host 10.1.1.2 5000
 ip netstream export source interface Vlan-interface10
#
ip netstream aggregation protocol-port
 enable
 ip netstream export host 10.1.1.2 5000
```

```
#
ip netstream aggregation tos-protocol-port
 enable
 ip netstream export host 10.1.1.2 5000
#
```

Example: Configuring IPv6 NetStream

Applicable product matrix

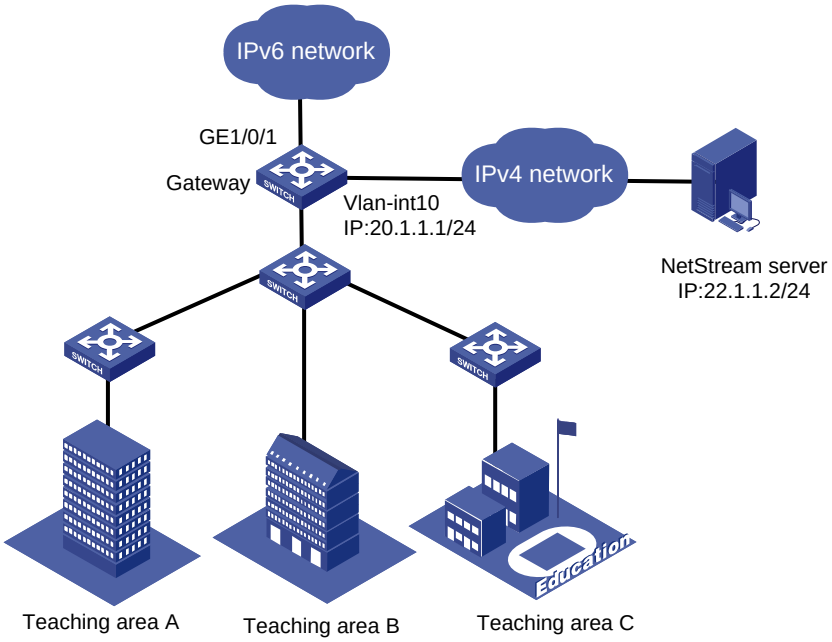
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 140, a school is divided into three teaching areas, each with the same bandwidth.

To deploy an IPv6 network, configure IPv6 NetStream on Gateway so the administrator can obtain information about bandwidth utilization for network planning and traffic monitoring.

Figure 140 Network diagram



Configuration restrictions and guidelines

When you configure IPv6 NetStream, follow these restrictions and guidelines:

- This section focuses on the description and configuration of Gateway that acts as an NDE.

- The destination UDP port number configured on Gateway must be the same as the UDP port number of the NetStream server.
- Configurations in IPv6 NetStream aggregation view only apply to aggregation data export. Configurations in system view apply to NetStream traditional data export.
- To reduce the bandwidth consumption of the NetStream data, merge the flows into one aggregation flow if each aggregation criterion is of the same value.

Configuration procedures

Enable IPv6 NetStream for incoming and outgoing traffic on GigabitEthernet 1/0/1.

```
<Gateway> system-view
[Gateway] ipv6
[Gateway] interface GigabitEthernet 1/0/1
[Gateway-GigabitEthernet1/0/1] ipv6 netstream inbound
[Gateway-GigabitEthernet1/0/1] ipv6 netstream outbound
[Gateway-GigabitEthernet1/0/1] quit
```

Specify an IP address for VLAN-interface 10.

```
[Gateway] vlan 10
[Gateway] interface vlan-interface 10
[Gateway-Vlan-interface10] ip address 20.1.1.1 255.255.255.0
[Gateway-Vlan-interface10] quit
```

Configure VLAN-interface 10 as the source interface for IPv6 NetStream data export.

```
[Gateway] ipv6 netstream export source interface Vlan-interface 10
```

Configure the destination address for IPv6 NetStream traditional data export as 22.1.1.2 with port 5000.

```
[Gateway] ipv6 netstream export host 22.1.1.2 5000
```

Set the aggregation mode as protocol-port. Configure the destination address for IPv6 NetStream traditional data export as 22.1.1.2 with port 5000.

```
[Gateway] ipv6 netstream aggregation protocol-port
[Gateway-ns6-aggregation-protport] ipv6 netstream export host 22.1.1.2 5000
[Gateway-ns6-aggregation-protport] enable
[Gateway-ns6-aggregation-protport] quit
```

Verifying the configuration

After the above configurations are completed, display the statistics of IPv6 NetStream data export.

```
[Gateway] display ipv6 netstream export
IPv6 export information:
  Stream source interface                      :
  Stream destination VPN-instance              :
  Stream destination IP (UDP)                  : 22.1.1.2 (5000)
  Version 9 exported stream number             : 0
  Version 9 exported UDP datagram number (failed): 0 (0)

protocol-port aggregation export information:
  Stream source interface                      :
```

```
  Stream destination VPN-instance                :
  Stream destination IP (UDP)                    : 22.1.1.2 (5000)
  Version 9 exported stream number               : 0
  Version 9 exported UDP datagram number (failed): 0 (0)
```

Configuration files

```
#
 ipv6
#
vlan 10
#
interface Vlan-interface10
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 ipv6 netstream inbound
 ipv6 netstream outbound
#
 ipv6 netstream export host 22.1.1.2 5000
 ipv6 netstream export source interface Vlan-interface10
#
ipv6 netstream aggregation protocol-port
 enable
 ipv6 netstream export host 22.1.1.2 5000
#
```

NQA configuration examples

This chapter provides NQA configuration examples.

Example: Configuring an ICMP echo operation

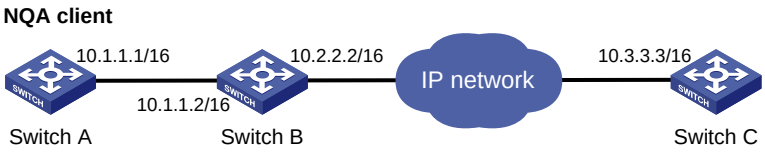
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 141, configure and schedule an ICMP echo operation from the NQA client Switch A to Switch C through Switch B to test the round-trip time.

Figure 141 Network diagram



Configurations restrictions and guidelines

When you configure an ICMP echo operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Create an ICMP echo operation, and specify 10.3.3.3 as the destination IP address.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type icmp-echo
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.3.3.3
```

Specify 10.1.1.2 as the next hop.

```
[SwitchA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
```

Configure the operation to repeat at an interval of 5000 milliseconds. If an operation is not completed when the interval is reached, the next operation does not start. (By default, the time interval is 0 milliseconds, and only one operation is performed.)

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 5000
```

Configure the ICMP echo operation to perform 10 probes.

```
[SwitchA-nqa-admin-test-icmp-echo] probe count 10
```

Enable saving history records, and configure the maximum number of history records that can be saved as 10.

```
[SwitchA-nqa-admin-test-icmp-echo] history-record enable
[SwitchA-nqa-admin-test-icmp-echo] history-record number 10
```

Start the ICMP echo operation.

```
[SwitchA-nqa-admin-test-icmp-echo] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the ICMP echo operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the ICMP echo operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.3.3.3
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 0/16/1
      Square-Sum of round trip time: 256
      Last succeeded probe time: 2012-08-23 15:00:01.2
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

Display the history records of the ICMP echo operations.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    370        10           Succeeded        2012-08-23 15:00:01.2
    369        10           Succeeded        2012-08-23 15:00:01.2
    368        10           Succeeded        2012-08-23 15:00:01.2
    367        10           Succeeded        2012-08-23 15:00:01.2
    366        4            Succeeded        2012-08-23 15:00:01.2
    365        10           Succeeded        2012-08-23 15:00:01.2
    364        10           Succeeded        2012-08-23 15:00:01.1
```

```
    363         10          Succeeded        2012-08-23 15:00:01.1
    362         10          Succeeded        2012-08-23 15:00:01.1
    361         4           Succeeded        2012-08-23 15:00:01.1
```

Configuration files

```
#
nqa entry admin test
 type icmp-echo
  destination ip 10.3.3.3
  frequency 5000
  history-record enable
  history-record number 10
  next-hop 10.1.1.2
  probe count 10
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a DHCP operation

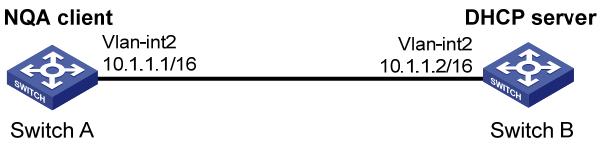
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 142, configure and schedule a DHCP operation to test the time for Switch A to obtain an IP address from the DHCP server Switch B.

Figure 142 Network diagram



Configurations restrictions and guidelines

When you configure a DHCP operation, follow these restrictions and guidelines:

- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

- The DHCP operation requires a DHCP server. It also requires a DHCP relay agent if the client and server are on different subnets. Configure the DHCP server before the operation starts.

Configuration procedures

Create a DHCP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dhcp
```

Specify VLAN-interface 2 as the operation interface.

```
[SwitchA-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-dhcp] history-record enable
```

Start the DHCP operation.

```
[SwitchA-nqa-admin-test-dhcp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the DHCP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the DHCP operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 624/624/624
      Square-Sum of round trip time: 389376
      Last succeeded probe time: 2012-11-22 09:56:03.2
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the DHCP operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          624          Succeeded        2012-11-22 09:56:03.2
```

Configuration files

```
#
nqa entry admin test
```

```
 type dhcp
  history-record enable
  operation interface Vlan-interface2
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a DNS operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 143:

- Configure a DNS operation to test whether Switch A can translate the domain name **host.com** into an IP address through the DNS server.
- Test the time required for the resolution.

Figure 143 Network diagram

Configurations restrictions and guidelines

When you configure a DNS operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Configure a DNS operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dns
```

Specify the IP address of the DNS server 10.2.2.2 as the destination address.

```
[SwitchA-nqa-admin-test-dns] destination ip 10.2.2.2
```

Specify the domain name to be translated as **host.com**.

```
[SwitchA-nqa-admin-test-dns] resolve-target host.com
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-dns] history-record enable
```

Start the DNS operation.

```
[SwitchA-nqa-admin-test-dns] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the DNS operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the DNS operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 62/62/62
      Square-Sum of round trip time: 3844
      Last succeeded probe time: 2012-11-10 10:49:37.3
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

Display the history records of the DNS operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          62           Succeeded        2012-11-10 10:49:37.3
```

Configuration files

```
#
nqa entry admin test
 type dns
  destination ip 10.2.2.2
  history-record enable
  resolve-target host.com
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring an FTP operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 144, configure an FTP operation to test the time for Switch A to upload a file to the FTP server Switch B. The login username is **admin**, the login password is **systemtest**, and the file to be transferred to the FTP server is **config.txt**.

Figure 144 Network diagram

Configurations restrictions and guidelines

When you configure an FTP operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.
- When you perform the FTP **put** operation, the NQA client will upload a newly created operation file named *file-name* of a fixed size to the FTP server, instead of uploading a file saved on the NQA client to the FTP server.
- Use a small file and specify a longer duration for the FTP operation. A large file might result in transfer failure because of timeout.

Configuration procedures

Create an FTP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type ftp
```

Specify the IP address of the FTP server 10.2.2.2 as the destination address.

```
[SwitchA-nqa-admin-test-ftp] destination ip 10.2.2.2
```

Specify 10.1.1.1 as the source IP address.

```
[SwitchA-nqa-admin-test-ftp] source ip 10.1.1.1
```

Specify **put** as the FTP operation type.

```
[SwitchA-nqa-admin-test-ftp] operation put
```

Specify **config.txt** as the name of a file to be transferred.

```
[SwitchA-nqa-admin-test-ftp] filename config.txt
```

Specify the FTP login username and password.

```
[SwitchA-nqa-admin-test-ftp] username admin
[SwitchA-nqa-admin-test-ftp] password systemtest
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-ftp] history-record enable
```

Start the FTP operation.

```
[SwitchA-nqa-admin-test-ftp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the FTP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the FTP operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 173/173/173
      Square-Sum of round trip time: 29929
      Last succeeded probe time: 2012-11-22 10:07:28.6
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the FTP operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1           173          Succeeded        2012-11-22 10:07:28.6
```

Configuration files

```
#
nqa entry admin test
 type ftp
```

```
  destination ip 10.2.2.2
  filename config.txt
  history-record enable
  operation put
  password systemtest
  source ip 10.1.1.1
  username admin
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring an HTTP operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 145, configure an HTTP operation on the NQA client to test the time for the client to obtain data from the HTTP server.

Figure 145 Network diagram

Configurations restrictions and guidelines

When you configure an HTTP operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Create an HTTP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type http
```

Specify the IP address of the HTTP server 10.2.2.2 as the destination address.

```
[SwitchA-nqa-admin-test-http] destination ip 10.2.2.2
```

Specify **index.htm** as the URL of the HTTP server.

```
[SwitchA-nqa-admin-test-http] url /index.htm
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-http] history-record enable
```

Start the HTTP operation.

```
[SwitchA-nqa-admin-test-http] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the HTTP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the HTTP operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 64/64/64
      Square-Sum of round trip time: 4096
      Last succeeded probe time: 2012-11-22 10:12:47.9
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the HTTP operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          64           Succeeded        2012-11-22 10:12:47.9
```

Configuration files

```
#
nqa entry admin test
 type http
  destination ip 10.2.2.2
  history-record enable
  url /index.htm
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a UDP jitter operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 146, configure a UDP jitter operation to test the jitter, delay, and round-trip time between Switch A and Switch B.

Figure 146 Network diagram

Configurations restrictions and guidelines

When you configure a UDP jitter operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You must configure Switch B as the NQA server before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Configuring Switch B

Enable the NQA server. Configure a listening service to listen to the IP address 10.2.2.2 and UDP port 9000.

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server udp-echo 10.2.2.2 9000
```

Configuring Switch A

Create a UDP jitter operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type udp-jitter
```

Configure 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[SwitchA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-udp-jitter] destination port 9000
```

Configure the operation to repeat at an interval of 1000 milliseconds.

```
[SwitchA-nqa-admin-test-udp-jitter] frequency 1000
[SwitchA-nqa-admin-test-udp-jitter] quit
```

Start the UDP jitter operation.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the UDP jitter operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

To verify UDP jitter operation results, use the **display nqa result** command or the **display nqa statistics** command. The **display nqa history** command does not display output for UDP jitter operations.

Display the results of the UDP jitter operation.

```
[SwitchA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 15/32/17
      Square-Sum of round trip time: 3235
      Last succeeded probe time: 2012-05-29 13:56:17.6
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 10
      Min positive SD: 4                   Min positive DS: 1
      Max positive SD: 21                  Max positive DS: 28
      Positive SD number: 5                Positive DS number: 4
      Positive SD sum: 52                  Positive DS sum: 38
      Positive SD average: 10              Positive DS average: 10
      Positive SD square sum: 754          Positive DS square sum: 460
      Min negative SD: 1                   Min negative DS: 6
      Max negative SD: 13                  Max negative DS: 22
      Negative SD number: 4                Negative DS number: 5
      Negative SD sum: 38                  Negative DS sum: 52
      Negative SD average: 10              Negative DS average: 10
      Negative SD square sum: 460          Negative DS square sum: 754
    One way results:
      Max SD delay: 15                     Max DS delay: 16
```

```
      Min SD delay: 7                         Min DS delay: 7
      Number of SD delay: 10                  Number of DS delay: 10
      Sum of SD delay: 78                     Sum of DS delay: 85
      Square sum of SD delay: 666             Square sum of DS delay: 787
      SD lost packet(s): 0                    DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
```

Display the UDP jitter operation statistics.

```
[SwitchA] display nqa statistics admin test
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 10.2.2.2
      Start time: 2012-05-29 13:56:14.0
      Life time: 47 seconds
      Send operation times: 410            Receive response times: 410
      Min/Max/Average round trip time: 1/93/19
      Square-Sum of round trip time: 206176
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 410
      Min positive SD: 3                      Min positive DS: 1
      Max positive SD: 30                     Max positive DS: 79
      Positive SD number: 186                 Positive DS number: 158
      Positive SD sum: 2602                   Positive DS sum: 1928
      Positive SD average: 13                 Positive DS average: 12
      Positive SD square sum: 45304           Positive DS square sum: 31682
      Min negative SD: 1                      Min negative DS: 1
      Max negative SD: 30                     Max negative DS: 78
      Negative SD number: 181                 Negative DS number: 209
      Negative SD sum: 181                    Negative DS sum: 209
      Negative SD average: 13                 Negative DS average: 14
      Negative SD square sum: 46994           Negative DS square sum: 3030
    One way results:
      Max SD delay: 46                        Max DS delay: 46
      Min SD delay: 7                         Min DS delay: 7
      Number of SD delay: 410                 Number of DS delay: 410
      Sum of SD delay: 3705                   Sum of DS delay: 3891
      Square sum of SD delay: 45987           Square sum of DS delay: 49393
      SD lost packet(s): 0                    DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
```

Configuration files

- Switch B:

```
#
 nqa server enable
 nqa server udp-echo 10.2.2.2 9000
```

- Switch A:

```
#
nqa entry admin test
 type udp-jitter
  destination ip 10.2.2.2
  destination port 9000
  frequency 1000
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring an SNMP operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 147, configure an SNMP operation to test the time for the NQA client to get a response packet from the SNMP agent Switch B.

Figure 147 Network diagram

Configurations restrictions and guidelines

When you configure an SNMP operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You must configure SNMP on Switch B before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Configuring Switch B (SNMP agent)

Enable the SNMP agent.

```
<SwitchB> system-view
[SwitchB] snmp-agent
```

Set the SNMP version to **all**, the read community to **public**, and the write community to **private**.

```
[SwitchB] snmp-agent sys-info version all
[SwitchB] snmp-agent community read public
[SwitchB] snmp-agent community write private
```

Configuring Switch A

Create an SNMP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type snmp
```

Configure the IP address of the SNMP agent 10.2.2.2 as the destination IP address.

```
[SwitchA-nqa-admin-test-snmp] destination ip 10.2.2.2
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-snmp] history-record enable
```

Start the SNMP operation.

```
[SwitchA-nqa-admin-test-snmp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the SNMP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the SNMP operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 50/50/50
      Square-Sum of round trip time: 2500
      Last succeeded probe time: 2012-11-22 10:24:41.1
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the SNMP operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          50           Timeout          2012-11-22 10:24:41.1
```

Configuration files

- Switch B:

```
#
 snmp-agent
 snmp-agent local-engineid 800063A20300E0FC123456
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
```

- Switch A:

```
#
nqa entry admin test
 type snmp
  destination ip 10.2.2.2
  history-record enable
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a TCP operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 148, configure a TCP operation to test the time for the NQA client Switch A to establish a TCP connection to the NQA server Switch B.

Figure 148 Network diagram

Configurations restrictions and guidelines

When you configure a TCP operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You must configure Switch B as the NQA server before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Configuring Switch B

Enable the NQA server.

```
<SwitchB> system-view
[SwitchB] nqa server enable
```

Configure a listening service to listen to the IP address 10.2.2.2 and TCP port 9000.

```
[SwitchB] nqa server tcp-connect 10.2.2.2 9000
```

Configuring Switch A

Create a TCP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type tcp
```

Specify 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[SwitchA-nqa-admin-test-tcp] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-tcp] destination port 9000
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-tcp] history-record enable
```

Start the TCP operation.

```
[SwitchA-nqa-admin-test-tcp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the TCP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the TCP operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 13/13/13
      Square-Sum of round trip time: 169
      Last succeeded probe time: 2012-11-22 10:27:25.1
    Extend results:
```

```
  Packet lost in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
```

Display the history records of the TCP operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          13             Succeeded        2012-11-22 10:27:25.1
```

Configuration files

- Switch B:

```
#
 nqa server enable
 nqa server tcp-connect 10.2.2.2 9000
```

- Switch A:

```
#
nqa entry admin test
 type tcp
  destination ip 10.2.2.2
  destination port 9000
  history-record enable
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a UDP echo operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 149, configure a UDP echo operation to test the round-trip time between Switch A and Switch B.

Figure 149 Network diagram

Configurations restrictions and guidelines

When you configure a UDP echo operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You must configure Switch B as the NQA server before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Configuring Switch B

Enable the NQA server.

```
<SwitchB> system-view
[SwitchB] nqa server enable
```

Configure a listening service to listen to the IP address 10.2.2.2 and UDP port 8000.

```
[SwitchB] nqa server udp-echo 10.2.2.2 8000
```

Configuring Switch A

Create a UDP echo operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type udp-echo
```

Specify 10.2.2.2 as the destination IP address and port 8000 as the destination port.

```
[SwitchA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-udp-echo] destination port 8000
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-udp-echo] history-record enable
```

Start the UDP echo operation.

```
[SwitchA-nqa-admin-test-udp-echo] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the UDP echo operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the UDP echo operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
```

```
  Destination IP address: 10.2.2.2
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 25/25/25
    Square-Sum of round trip time: 625
    Last succeeded probe time: 2012-11-22 10:36:17.9
  Extend results:
    Packet lost in test: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to sequence error: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the history records of the UDP echo operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1           25            Succeeded        2012-11-22 10:36:17.9
```

Configuration files

- Switch B:

```
#
 nqa server enable
 nqa server udp-echo 10.2.2.2 8000
```

- Switch A:

```
#
nqa entry admin test
 type udp-echo
  destination ip 10.2.2.2
  destination port 8000
  history-record enable
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a voice operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 150, configure a voice operation to test jitters and voice quality for voice packets between Switch A and Switch B.

Figure 150 Network diagram

Configurations restrictions and guidelines

When you configure a voice operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you perform the configuration.
- You must configure Switch B as the NQA server before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Configuring Switch B

Enable the NQA server.

```
<SwitchB> system-view
[SwitchB] nqa server enable
```

Configure a listening service to listen to IP address 10.2.2.2 and UDP port 9000.

```
[SwitchB] nqa server udp-echo 10.2.2.2 9000
```

Configuring Switch A

Create a voice operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type voice
```

Specify 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[SwitchA-nqa-admin-test-voice] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-voice] destination port 9000
[SwitchA-nqa-admin-test-voice] quit
```

Start the voice operation.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the voice operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

To verify voice operation results, use the **display nqa result** command or the **display nqa statistics** command. The **display nqa history** command does not display output for voice operations.

Display the results of the voice operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1000          Receive response times: 1000
      Min/Max/Average round trip time: 31/1328/33
      Square-Sum of round trip time: 2844813
      Last succeeded probe time: 2012-06-13 09:49:31.1
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 1000
      Min positive SD: 1                  Min positive DS: 1
      Max positive SD: 204                Max positive DS: 1297
      Positive SD number: 257             Positive DS number: 259
      Positive SD sum: 759                Positive DS sum: 1797
      Positive SD average: 2              Positive DS average: 6
      Positive SD square sum: 54127       Positive DS square sum: 1691967
      Min negative SD: 1                  Min negative DS: 1
      Max negative SD: 203                Max negative DS: 1297
      Negative SD number: 255             Negative DS number: 259
      Negative SD sum: 759                Negative DS sum: 1796
      Negative SD average: 2              Negative DS average: 6
      Negative SD square sum: 53655       Negative DS square sum: 1691776
    One way results:
      Max SD delay: 343                   Max DS delay: 985
      Min SD delay: 343                   Min DS delay: 985
      Number of SD delay: 1               Number of DS delay: 1
      Sum of SD delay: 343                Sum of DS delay: 985
      Square sum of SD delay: 117649      Square sum of DS delay: 970225
      SD lost packet(s): 0                DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
    Voice scores:
      MOS value: 4.38                     ICPIF value: 0
```

Display the statistics of the voice operation.

```
[SwitchA] display nqa statistics admin test
```

```
NQA entry(admin admin, tag test) test statistics:
  NO. : 1
  Destination IP address: 10.2.2.2
    Start time: 2012-06-13 09:45:37.8
    Life time: 331
    Send operation times: 4000           Receive response times: 4000
    Min/Max/Average round trip time: 15/1328/32
    Square-Sum of round trip time: 7160528
  Extended results:
    Packet lost in test: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to sequence error: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packet(s) arrived late: 0
  Voice results:
   RTT number: 4000
    Min positive SD: 1                   Min positive DS: 1
    Max positive SD: 360                 Max positive DS: 1297
    Positive SD number: 1030             Positive DS number: 1024
    Positive SD sum: 4363                Positive DS sum: 5423
    Positive SD average: 4               Positive DS average: 5
    Positive SD square sum: 497725       Positive DS square sum: 2254957
    Min negative SD: 1                   Min negative DS: 1
    Max negative SD: 360                 Max negative DS: 1297
    Negative SD number: 1028             Negative DS number: 1022
    Negative SD sum: 1028                Negative DS sum: 1022
    Negative SD average: 4               Negative DS average: 5
    Negative SD square sum: 495901       Negative DS square sum: 5419
  One way results:
    Max SD delay: 359                    Max DS delay: 985
    Min SD delay: 0                      Min DS delay: 0
    Number of SD delay: 4                Number of DS delay: 4
    Sum of SD delay: 1390                Sum of DS delay: 1079
    Square sum of SD delay: 483202       Square sum of DS delay: 973651
    SD lost packet(s): 0                 DS lost packet(s): 0
    Lost packet(s) for unknown reason: 0
  Voice scores:
    Max MOS value: 4.38                  Min MOS value: 4.38
    Max ICPIF value: 0                   Min ICPIF value: 0
```

Configuration files

- Switch B:

```
#
 nqa server enable
```

```
 nqa server udp-echo 10.2.2.2 8000
```

- Switch A:

```
#
nqa entry admin test
 type voice
  destination ip 10.2.2.2
  destination port 9000
#
 nqa schedule admin test start-time now lifetime forever
```

Example: Configuring a DLSw operation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 151, configure a DLSw operation to test the response time of the DLSw device.

Figure 151 Network diagram

Configurations restrictions and guidelines

When you configure a DLSw operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you perform the configuration.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or when the operation has finished.

Configuration procedures

Create a DLSw operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dlsw
```

Specify 10.2.2.2 as the destination IP address.

```
[SwitchA-nqa-admin-test-dlsw] destination ip 10.2.2.2
```

Enable the saving of history records.

```
[SwitchA-nqa-admin-test-dlsw] history-record enable
```

Start the DLSw operation.

```
[SwitchA-nqa-admin-test-dlsw] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

After the DLSw operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

Verifying the configuration

Display the results of the DLSw operation.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 19/19/19
      Square-Sum of round trip time: 361
      Last succeeded probe time: 2012-11-22 10:40:27.7
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the DLSw operation.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          19           Succeeded        2012-11-22 10:40:27.7
```

Configuration files

```
#
nqa entry admin test
 type dlsw
  destination ip 10.2.2.2
  history-record enable
#
 nqa schedule admin test start-time now lifetime forever
```

NTP configuration examples

This chapter provides NTP configuration examples.

Table 14 NTP association modes

Mode	Clock source	Time accuracy	Principles
Client/server	• A client synchronizes to a server. • A client can synchronize to multiple time servers.	High	• Configure only the client. • A client and a server can be in the same subnet or in different subnets. • A client can synchronize to a server, but a server cannot synchronize to a client. • Specify the IP address for the server on each client when the IP address of the reference source changes. • Applicable to a network environment when the reference source is stable.
Symmetric active/passive	• A symmetric active peer and a symmetric passive peer can synchronize to each other. If both of them are synchronized, the peer with a higher stratum synchronizes to the peer with a lower stratum. • An active peer can synchronize to multiple passive peers.	High	• Configure only the active peer. • A symmetric active peer and a symmetric passive peer can be in the same subnet or in different subnets. • A symmetric active peer and a symmetric passive peer can synchronize to each other.
Broadcast	When a client receives the first broadcast message from a server, if the stratum in the message is lower than the stratum of the client, the client uses the server as the clock source and synchronizes its clock to the server. Otherwise, the client uses its own clock.	Low	• Configure both the client and server. • A client and a server must be in the same subnet. • Configure NTP only on the server if the IP address of the clock source changes. • The broadcast mode is intended for configurations involving one or a few servers and a potentially large client population.

Mode	Clock source	Time accuracy	Principles
Multicast	When a client receives the first multicast message from a server, if the stratum in the message is lower than the stratum of the client, the client uses the server as the clock source and synchronizes its clock to the server. Otherwise, the client uses its own clock.	Low	• Configure both the client and server. • A client and a server can be in the same subnet or in different subnets. If they are in different subnets, they must support multicast protocols. • Configure only the server when the reference source changes. • The broadcast mode is intended for configurations involving one or a few servers and a potentially large client population.

Example: Configuring the NTP client/server mode

Applicable product matrix

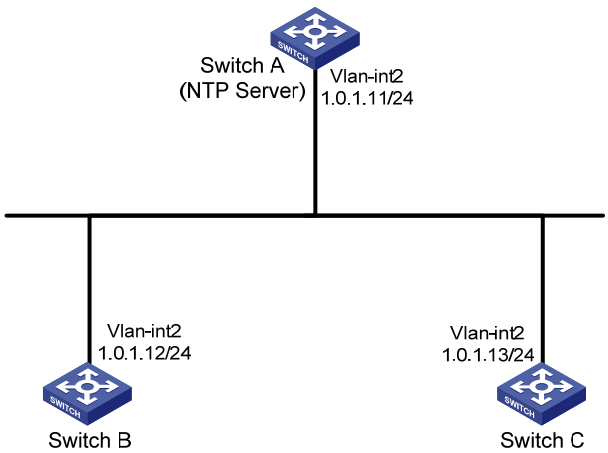
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 152, configure NTP to meet the following requirements:

- Switch A's local clock is a reference source, with the stratum level 2.
- Switch B and Switch C operate in client mode.
- Switch A is the NTP server for Switch B and Switch C.

Figure 152 Network diagram



Configuration procedures

Specify the local clock as the reference source, with the stratum level 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] ntp-service refclock-master 2
```

Specify Switch A as the NTP server of Switch B.

```
<SwitchB> system-view
[SwitchB] ntp-service unicast-server 1.0.1.11
```

Specify Switch A as the NTP server of Switch C:

```
<SwitchC> system-view
[SwitchC] ntp-service unicast-server 1.0.1.11
```

Verifying the configuration

Display the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 2.02 ms
 Root dispersion: 1.05 ms
 Peer dispersion: 7.81 ms
 Reference time: 13:44:48.615 UTC Mar 23 2013(D4F83050.9D975F2C)
```

The output shows that Switch B has synchronized to Switch A. The clock stratum level is 3 on Switch B and 2 on Switch A.

Display NTP association information for Switch B.

```
[SwitchB] display ntp-service sessions
        source       reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345] 1.0.1.11     127.127.1.0        2     3   64   48   -1.3    2.3    0.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

The output shows that an association has been established between Switch B and Switch A.

Configuration files

- Switch A:

  ```
  #
   ntp-service refclock-master 2
  ```

- Switch B:

  ```
  #
  ```

```
 ntp-service unicast-server 1.0.1.11
```

- Switch C:

```
#
 ntp-service unicast-server 1.0.1.11
```

Example: Configuring the NTP symmetric active/passive mode

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

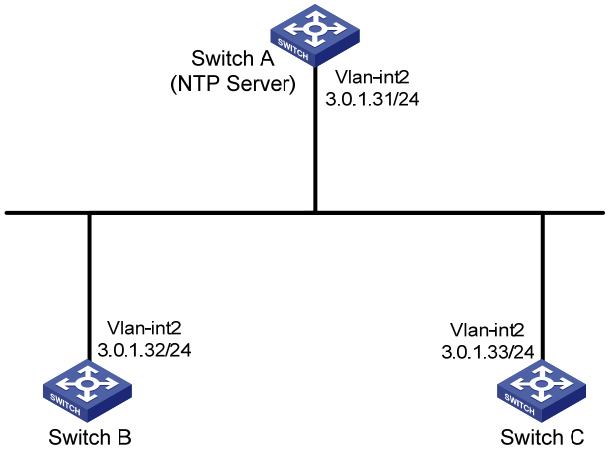
Network requirements

As shown in Figure 153, configure NTP to meet the following requirements:

- Switch A's local clock is a reference source, with the stratum level 2.
- Switch B operates in client mode, and Switch A is the NTP server for Switch B.
- Switch C operates in symmetric-active mode, and Switch B is the passive peer of Switch C.

When Switch A fails, Switch B and Switch C can operate as a backup for each other.

Figure 153 Network diagram



Configuration procedures

Specify the local clock as the reference source, with the stratum level 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] ntp-service refclock-master 2
```

Specify Switch A as the NTP server of Switch B.

```
<SwitchB> system-view
[SwitchB] ntp-service unicast-server 3.0.1.31
```

Display the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: -0.2118 ms
 Root delay: 2.68 ms
 Root dispersion: 775.15 ms
 Peer dispersion: 34.29 ms
 Reference time: 14:08:20.264 UTC Mar 23 2013(D4F835D4.43AB862B)
```

The output shows that Switch B has synchronized to Switch A. The clock stratum level is 3 on Switch B and 2 on Switch A.

Specify Switch A as the NTP server of Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service unicast-server 3.0.1.31
```

Configure Switch B as a symmetric passive peer of Switch C.

```
[SwitchC] ntp-service unicast-peer 3.0.1.32
```

Verifying the configuration

Disconnect Switch A from the network. Display the NTP status of Switch C after clock synchronization.

```
[SwitchC] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 3.0.1.32
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: -21.1982 ms
 Root delay: 15.00 ms
 Root dispersion: 775.15 ms
 Peer dispersion: 34.29 ms
 Reference time: 14:14:43.743 UTC Mar 23 2013(D4F83753.BE46F156)
```

The output shows that Switch C has synchronized to Switch B. The clock stratum level is 4 on Switch C and 3 on Switch B.

Configuration files

- Switch A:

  ```
  #
  ```

```
 ntp-service refclock-master 2
```

- Switch B:

```
#
 ntp-service unicast-server 3.0.1.31
```

- Switch C:

```
#
 ntp-service unicast-server 3.0.1.31
 ntp-service unicast-peer 3.0.1.32
```

Example: Configuring the NTP broadcast mode

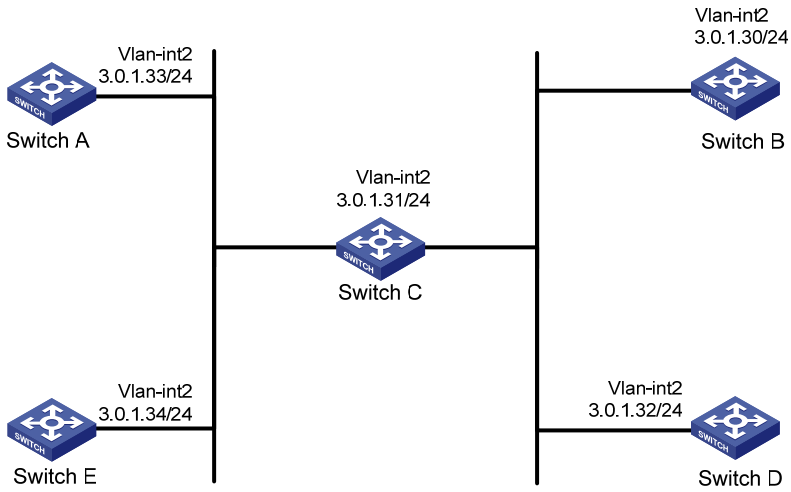
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 154, configure NTP to synchronize the time among multiple devices on a subnet.

Figure 154 Network diagram



Configuration procedures

Specify the local clock as the reference source, with the stratum level 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

Configure Switch C to operate in broadcast server mode and send broadcast messages through VLAN-interface 2.

```
[SwitchC] interface Vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server
```

Configure Switch A to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

Configure Switch B, Switch D, and Switch E in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

Display the NTP status of Switch A after clock synchronization.

```
[SwitchA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.0222 ms
 Root delay: 2.28 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 14:14:43.743 UTC Mar 23 2013(D4F83753.BE46F156)
```

The output shows that Switch A has synchronized to Switch C. The clock stratum level is 3 on Switch A and 2 on Switch C.

Display NTP association information for Switch A.

```
[SwitchA-Vlan-interface2] display ntp-service sessions
      source    reference      stra  reach  poll  now offset   delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0      2    254    64   62  -16.0    32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

The output shows that an association has been set up between Switch A and Switch C.

Configuration files

- Switch C:

```
#
 ntp-service refclock-master 2
#
interface Vlan-interface2
 ntp-service broadcast-server
```

- Switch A:

```
#
interface Vlan-interface2
 ntp-service broadcast-client
```

- Switch B:

```
#
interface Vlan-interface2
 ntp-service broadcast-client
```

- Switch D:

```
#
interface Vlan-interface2
 ntp-service broadcast-client
```

- Switch E:

```
#
interface Vlan-interface2
 ntp-service broadcast-client
```

Example: Configuring the NTP multicast mode

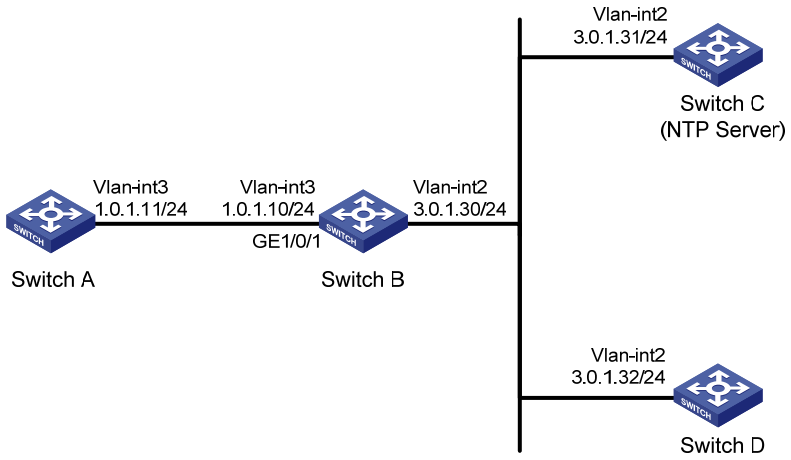
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 155, configure NTP to synchronize the time among multiple devices on different subnets.

Figure 155 Network diagram



Configuration procedures

Specify the local clock as the reference source, with the stratum level 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

Configure Switch C to operate in multicast server mode and send multicast messages through VLAN-interface 2.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

Configure Switch D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

Configure multicast functions on Switch B.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim dm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port GigabitEthernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] igmp enable
[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1
[SwitchB-Vlan-interface3] quit
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

Switch A and Switch C are not on the same subnet, so you need to perform the following step. Otherwise, Switch A cannot receive multicast messages sent by Switch C.

Configure Switch A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

Verifying the configuration

Display the NTP status of Switch A after clock synchronization.

```
[SwitchA-Vlan-interface3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 40.00 ms
 Root dispersion: 10.83 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:30:57.077 UTC Mar 23 2013(D4F85741.13F0AA21)
```

The output shows that Switch A has synchronized to Switch C. The clock stratum level is 3 on Switch A and 2 on Switch C.

Configuration files

- Switch A:

```
#
 ntp-service refclock-master 2
#
interface Vlan-interface3
 ntp-service multicast-client
```

- Switch B:

```
#
 multicast routing-enable
#
interface Vlan-interface2
 pim dm
#
interface Vlan-interface3
 igmp enable
 igmp static-group 224.0.1.1
#
interface GigabitEthernet1/0/1
 port access vlan 3
 igmp-snooping static-group 224.0.1.1 vlan 3
```

- Switch C:

```
#
ntp-service refclock-master 2
#
interface Vlan-interface2
 ntp-service multicast-server
```

- Switch D:

```
#
interface Vlan-interface2
 ntp-service multicast-client
```

Example: Configuring the NTP broadcast mode with authentication

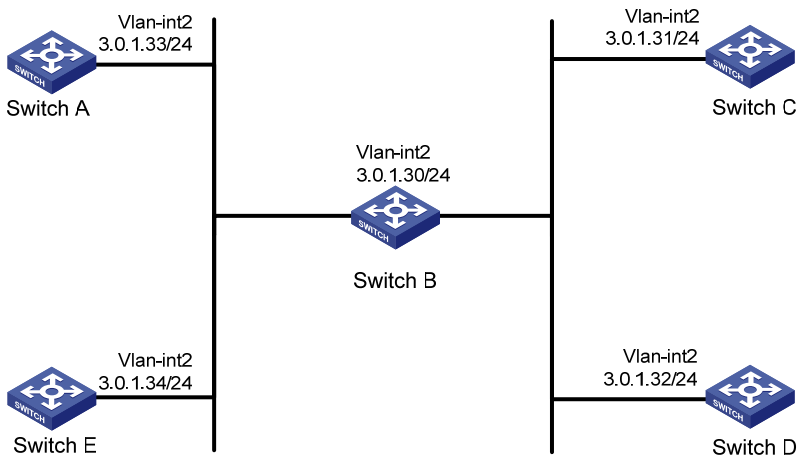
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 156, configure NTP to synchronize the time among multiple devices on a subnet. Configure NTP authentication to prevent attacks.

Figure 156 Network diagram



Configuration procedures

1. Configure Switch C:

Specify the local clock as the reference source, with the stratum level 2.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

Enable NTP authentication.

```
[SwitchC] ntp-service authentication enable
```

Configure an NTP authentication key in plain text. The key ID is **88**, and the key value is **123456**.

```
[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

Specify the key as trustworthy.

```
[SwitchC] ntp-service reliable authentication-keyid 88
```

Specify Switch C as an NTP broadcast server, and associate key **88** with Switch C.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

2. Configure Switch A:

Enable NTP authentication on Switch A.

```
<SwitchA> system-view
[SwitchA] ntp-service authentication enable
```

Configure an NTP authentication key in plain text. The key ID is **88**, and the key value is **123456**.

```
[SwitchA] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

Specify the key as trustworthy.

```
[SwitchA] ntp-service reliable authentication-keyid 88
```

Configure Switch A to operate in NTP broadcast client mode and receive NTP broadcast messages on VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

3. Configure Switch B, Switch D, and Switch E in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

Display NTP service status on Switch A.

```
[SwitchA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:30:57.077 UTC Mar 23 2013(D4F85741.13F0AA21)
```

The output shows that Switch A has synchronized to Switch C. The clock stratum level is 3 on Switch A and 2 on Switch C.

Configuration files

- Switch C:

```
#
interface Vlan-interface2
 ntp-service broadcast-server authentication-keyid 88
#
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5
OUM!K%F<+$[Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 88
 ntp-service refclock-master 3
#
```

- Switch A, Switch B, Switch D, and Switch E:

```
#
interface Vlan-interface2
 ntp-service broadcast-client
#
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5
OUM!K%F<+$[Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 88
#
```

OSPF configuration examples

This chapter provides OSPF configuration examples.

Example: Configuring basic OSPF

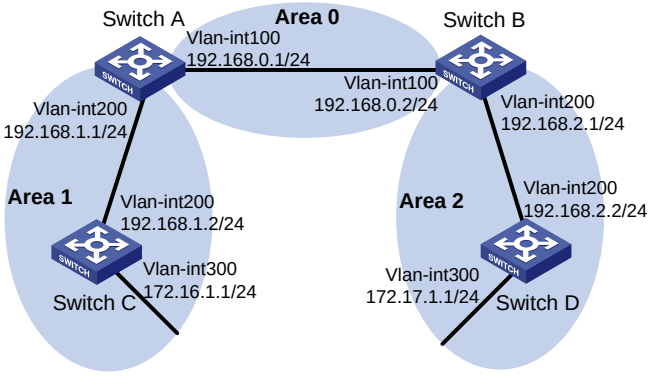
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 157, configure OSPF on the switches and split the AS into three OSPF areas.

Figure 157 Network diagram



Configuration restrictions and guidelines

OSPF uses a router ID to identify a switch. Make sure each switch in an AS has a unique router ID.

Configuration procedures

1. Configure IP addresses for the interfaces, as shown in Figure 157. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] router id 192.168.1.1
[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> system-view
[SwitchB] router id 192.168.2.1
[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> system-view
[SwitchC] router id 192.168.1.2
[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> system-view
[SwitchD] router id 192.168.2.2
[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
```

Verifying the configuration

Display information about OSPF neighbors on Switch A.

```
[SwitchA] display ospf peer verbose

          OSPF Process 1 with Router ID 192.168.1.1
                  Neighbors

 Area 0.0.0.0 interface 192.168.0.1(Vlan-interface 100)'s neighbors
 Router ID: 192.168.2.1      Address: 192.168.0.2      GR State: Normal
```

```
  State: Full  Mode:Nbr is  Master  Priority: 1
  DR: 192.168.0.2   BDR: 192.168.0.1   MTU: 0
  Dead timer due in 36  sec
  Neighbor is up for 00:15:04
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 3

                Neighbors

Area 0.0.0.1 interface 192.168.1.1(Vlan-interface 200)'s neighbors
Router ID: 192.168.1.2       Address: 192.168.1.2      GR State: Normal
  State: Full  Mode:Nbr is  Slave  Priority: 1
  DR: 192.168.1.2   BDR: 192.168.1.1   MTU: 0
  Dead timer due in 39  sec
  Neighbor is up for 00:07:32
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2
```

The output shows that Switch A has established OSPF neighbor relationships with Switch B and Switch C.

Display OSPF routing information on Switch A.

```
[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
 172.16.1.0/24      1563  Stub       192.168.1.2     172.16.1.1      0.0.0.1
 172.17.1.0/24      3125  Inter      192.168.0.2     192.168.2.1     0.0.0.0
 192.168.1.0/24     1562  Transit    192.168.1.1     192.168.0.1     0.0.0.1
 192.168.2.0/24     3124  Inter      192.168.0.2     192.168.2.1     0.0.0.0
 192.168.0.0/24     1562  Transit    192.168.0.1     192.168.0.1     0.0.0.0

 Total Nets: 5
 Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

Display OSPF routing information on Switch D.

```
[SwitchD] display ospf routing
          OSPF Process 1 with Router ID 192.168.2.2
                   Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.0/24      4687  Inter      192.168.2.1     192.168.2.1     0.0.0.2
 172.17.1.0/24      1     Stub       172.17.1.1      192.168.2.2     0.0.0.2
 192.168.1.0/24     4686  Inter      192.168.2.1     192.168.2.1     0.0.0.2
 192.168.2.0/24     1562  Transit    192.168.2.2     192.168.2.2     0.0.0.2
 192.168.0.0/24     3124  Inter      192.168.2.1     192.168.2.1     0.0.0.2
```

```
 Total Nets: 5
 Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0
```

On Switch D, ping the IP address 172.16.1.1 to test reachability.

```
[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
```

The output shows that the destination is reachable.

Configuration files

- Switch A:

```
#
 router id 192.168.1.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
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
#
```

- Switch B:

```
#
 router id 192.168.2.1
#
vlan 100
#
vlan 200
```

```
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
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
#
```

- Switch C:

```
#
 router id 192.168.1.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
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
#
```

- Switch D:

```
#
 router id 192.168.2.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
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
#
```

Example: Configuring an OSPF stub area

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

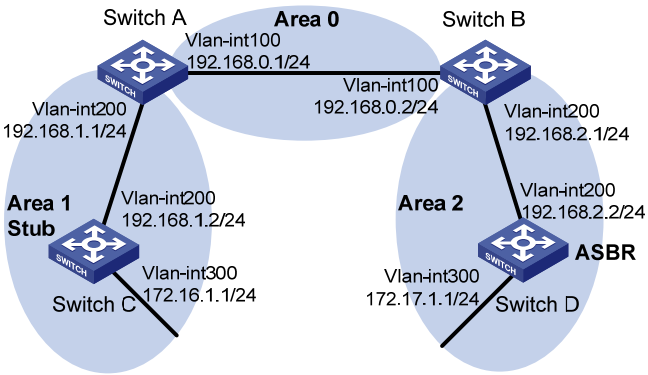
Network requirements

As shown in Figure 158, Switch D acts as the ASBR to redistribute external routes.

Configure OSPF to meet the following requirements:

- Run OSPF on the switches so that they can reach each other at the network layer.
- Configure Area 1 as a stub area to reduce the routing table size and LSAs.
- To further reduce the routing table size and advertised LSAs, configure the stub area as a totally stub area. The totally stub area will not import inter-area routes or external routes.

Figure 158 Network diagram



Configuration restrictions and guidelines

When you configure an OSPF stub area, follow these restrictions and guidelines:

- To configure a stub area, configure the **stub** command on all the switches attached to the area.
- To configure a totally stub area, configure the **stub** command on all the switches attached to the area, and configure the **stub no-summary** command on the ABR.

Configuration procedures

1. Configure IP addresses for the interfaces, as shown in Figure 158. (Details not shown.)
2. Enable OSPF (see "Example: Configuring basic OSPF").
3. Configure route redistribution:

   # Configure Switch D to redistribute static routes.

```
[SwitchD] ip route-static 200.0.0.0 8 null 0
[SwitchD] ospf
[SwitchD-ospf-1] import-route static
[SwitchD-ospf-1] quit
```

   # Display OSPF routing information on Switch C.

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 192.168.1.2
                   Routing Tables

 Routing for Network
 Destination       Cost  Type      NextHop         AdvRouter      Area
 172.16.1.0/24      1     Stub     172.16.1.1      172.16.1.1      0.0.0.1
 172.17.1.0/24      4687  Inter    192.168.1.1     192.168.0.1     0.0.0.1
 192.168.1.0/24     1562  Transit  192.168.1.2     172.16.1.1      0.0.0.1
 192.168.2.0/24     4686  Inter    192.168.1.1     192.168.0.1     0.0.0.1
 192.168.0.0/24     3124  Inter    192.168.1.1     192.168.0.1     0.0.0.1

 Routing for ASEs
 Destination       Cost     Type      Tag       NextHop        AdvRouter
 200.0.0.0/8        10      Type2      1        192.168.1.1     172.17.1.1

 Total Nets: 6
 Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

   The output shows that Switch C's routing table contains an AS external route when Switch C resides in a normal OSPF area.

4. Configuring Area 1 as a stub area:

   # Configure Switch A.

```
[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 Switch C.

```
[SwitchC] ospf
[SwitchC-ospf-1] stub-router
[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
```

Verifying the configuration

Display OSPF routing information on Switch C.

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Tables

 Routing for Network
 Destination       Cost  Type      NextHop         AdvRouter      Area
 0.0.0.0/0          65536 Inter      192.168.1.1     192.168.0.1     0.0.0.1
 172.16.1.0/24      1     Stub       172.16.1.1      172.16.1.1      0.0.0.1
 172.17.1.0/24      68660 Inter      192.168.1.1     192.168.0.1     0.0.0.1
 192.168.1.0/24     1562  Transit    192.168.1.2     172.16.1.1      0.0.0.1
 192.168.2.0/24     68659 Inter      192.168.1.1     192.168.0.1     0.0.0.1
 192.168.0.0/24     67097 Inter      192.168.1.1     192.168.0.1     0.0.0.1

 Total Nets: 6
 Intra Area: 2  Inter Area: 4  ASE: 0  NSSA: 0
```

The output shows that a default route has replaced the AS external route after the area where Switch C resides is configured as a stub area.

Configure the area as a totally stub area by filtering Type-3 LSAs out of 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
```

Display OSPF routing information on Switch C.

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 172.16.1.1
                  Routing Tables

 Routing for Network
 Destination       Cost  Type      NextHop         AdvRouter      Area
 0.0.0.0/0          1563  Inter      192.168.1.1     192.168.0.1     0.0.0.1
 172.16.1.0/24      1     Stub       172.16.1.1      172.16.1.1      0.0.0.1
 192.168.1.0/24     1562  Transit    192.168.1.2     172.16.1.1      0.0.0.1

 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

The output shows that inter-area routes have been removed, and only one external route (a default route) exists.

Configuration files

- Switch A:

```
#
 router id 192.168.1.1
```

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
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
#
```

- Switch B:

```
#
 router id 192.168.2.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
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
#
```

- Switch C:

```
#
 router id 192.168.1.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
```

```
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
ospf 1
 stub-router
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
  stub
#
```

- Switch D:

```
#
 router id 192.168.2.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
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
 import-route static
#
 ip route-static 200.0.0.0 255.0.0.0 NULL0
#
```

Example: Configuring an OSPF NSSA area

An NSSA area does not import AS external LSAs (Type-5 LSAs) but can import Type-7 LSAs generated by the NSSA ASBR. The NSSA ABR translates Type-7 LSAs into Type-5 LSAs and advertises the Type-5 LSAs to other areas.

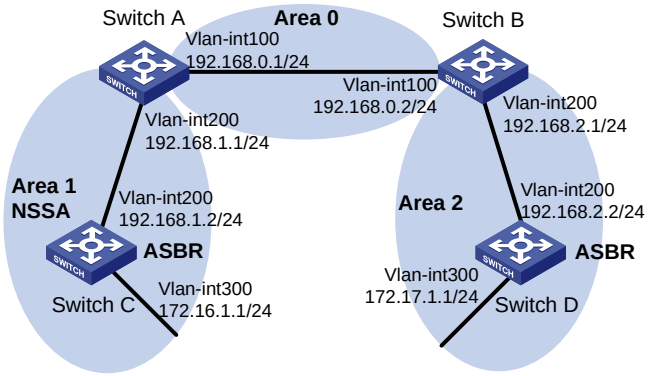
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 159, configure Area 1 as an NSSA area, and configure Switch C to advertise redistributed external routes to other areas within the AS.

Figure 159 Network diagram



Configuration restrictions and guidelines

When you configure an OSPF NSSA area, follow these restrictions and guidelines:

- To configure a stub area as an NSSA area, first remove the stub configuration by using the **undo stub** command.
- To configure an NSSA area, configure the **nssa** command on all the switches attached to the area.
- Virtual links are not allowed in NSSA areas.

Configuration procedures

1. Configure IP addresses for the interfaces, as shown in Figure 159. (Details not shown.)
2. Enable OSPF (see "Example: Configuring basic OSPF").
3. Configure OSPF to redistribute static routes on Switch D (see "Example: Configuring an OSPF stub area").
4. Configuring Area 1 as an NSSA area:

   # Configure Switch A.

   ```
   [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-0.0.0.0] quit
   [SwitchA-ospf-1] quit
   ```

   # Configure Switch C.

   ```
   [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
   ```

NOTE:

- To allow Switch C in the NSSA area to reach other ASs, configure the **nssa** command with the keyword **default-route-advertise** on Switch A (the ABR). This configuration allows Switch C to obtain a default route.
- Configuring the **nssa** command with the keyword **no-summary** on Switch A can reduce the routing table size on NSSA switches. On Switch C, you only need to configure the **nssa** command.

Display OSPF routing information on Switch C.

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 172.16.1.1
                  Routing Tables

 Routing for Network
 Destination       Cost  Type      NextHop         AdvRouter       Area
 0.0.0.0/0          1563  Inter      192.168.1.1     192.168.0.1     0.0.0.1
 172.16.1.0/24      1     Stub       172.16.1.1      172.16.1.1      0.0.0.1
 192.168.1.0/24     1562  Stub       192.168.1.2     172.16.1.1      0.0.0.1

 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

The output shows that the routing table of Switch C contains only a default route to reach other ASs.

Configure Switch C to redistribute a static route destined for network 100.0.0.0/8.

```
[SwitchC] ip route-static 100.0.0.0 8 null 0
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

Verifying the configuration

Display OSPF routing information on Switch D.

```
[SwitchD-ospf-1] display ospf routing
          OSPF Process 1 with Router ID 172.17.1.1
                  Routing Tables

 Routing for Network
 Destination       Cost  Type       NextHop         AdvRouter       Area
 172.16.1.0/24      4687  Inter      192.168.2.1     192.168.0.2     0.0.0.2
 172.17.1.0/24      1     Transit    172.17.1.1      172.17.1.1      0.0.0.2
 192.168.1.0/24     4686  Inter      192.168.2.1     192.168.0.2     0.0.0.2
 192.168.2.0/24     1562  Transit    192.168.2.2     172.17.1.1      0.0.0.2
 192.168.0.0/24     3124  Inter      192.168.2.1     192.168.0.2     0.0.0.2
 Routing for ASEs
 Destination       Cost     Type       Tag         NextHop         AdvRouter
 100.0.0.0/8       10       Type2      1           192.168.2.1     192.168.0.1

 Routing for NSSAs
```

```
Destination        Cost      Type       Tag         NextHop         AdvRouter

Total Nets: 6
Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

The output shows that the AS external route redistributed by the NSSA ASBR has been advertised to Area 2.

Configuration files

- Switch A:

```
#
 router id 192.168.1.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
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
#
```

- Switch B:

```
#
 router id 192.168.2.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
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
#
```

- Switch C:

```
#
 router id 192.168.1.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
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
  nssa
 import-route static
#
 ip route-static 100.0.0.0 255.0.0.0 NULL0
#
```

- Switch D:

```
#
 router id 192.168.2.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
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
 import-route static
#
 ip route-static 200.0.0.0 255.0.0.0 NULL0
#
```

Example: Configuring OSPF for a branch network

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 160:

- Distribution switches Switch A and Switch B connect the branch networks.
- Core switches Switch C and Switch D connect the external IP network, and they run BGP.
- Switch A and Switch B each provide dual uplinks to the two core switches for backup.

Configure the switches to make sure the branch networks and the external network can reach each other.

To reduce the LSDB size, configure route summarization on Switch A and Switch B.

Configure the gateway of hosts in each branch network as the IP address of the switch's VLAN interface that connects to the hosts.

Figure 160 Network diagram

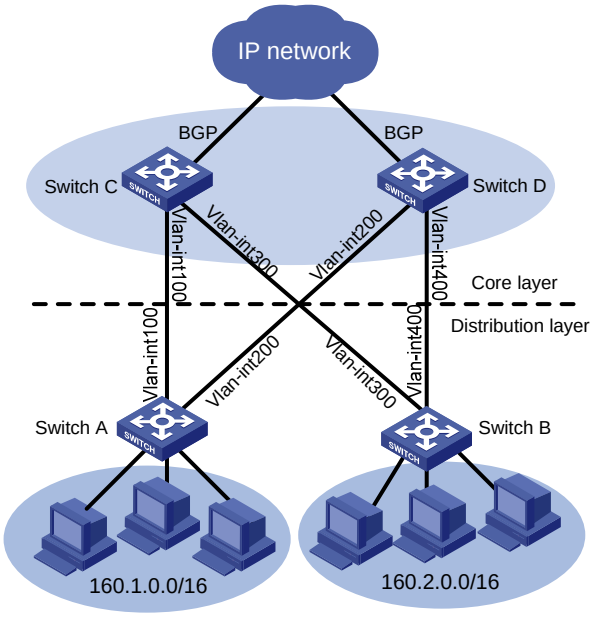


Table 15 IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.1.1.1/24	Switch C	Vlan-int100	10.1.1.2/24
	Vlan-int200	10.1.2.1/24		Vlan-int300	10.1.3.2/24

Switch B	Vlan-int300	10.1.3.1/24	Switch D	Vlan-int200	10.1.2.2/24
	Vlan-int400	10.1.4.1/24		Vlan-int400	10.1.4.2/24

Requirements analysis

For the switches to learn complete routes in the network, you must do the following:

- For Switch C and Switch D to learn the routes to the branch networks, configure OSPF to redistribute the branch networks on Switch A and Switch B.
- For Switch A and Switch B to learn routes to the external network, configure Switch C and Switch D to redistribute BGP routes into OSPF.

Configuration procedures

This configuration example describes only OSPF-related configurations. For information about BGP route learning and route redistribution, see *Layer 3—IP Routing Configuration Guide*.

1. Configure IP addresses for interfaces, as shown in Figure 160. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf
[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 10.1.2.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

   # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

   # Configure Switch D.

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
```

```
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Display routing information on Switch A. (In this example, Switch A connects three branch networks.)

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 14       Routes : 14

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan100
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.2.0/24         Direct 0    0            10.1.2.1        Vlan200
10.1.2.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.3.0/24         OSPF   10   2            10.1.1.2        Vlan100
10.1.4.0/24         OSPF   10   2            10.1.2.2        Vlan200
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
160.1.1.0/24        Direct 0    0            160.1.1.1       Vlan1
160.1.1.1/32        Direct 0    0            127.0.0.1       InLoop0
160.1.2.0/24        Direct 0    0            160.1.2.1       Vlan2
160.1.2.1/32        Direct 0    0            127.0.0.1       InLoop0
160.1.3.0/24        Direct 0    0            160.1.3.1       Vlan3
160.1.3.1/32        Direct 0    0            127.0.0.1       InLoop0
```

3. Configure route redistribution:

Configure OSPF to redistribute direct routes on Switch A, and configure Switch A to advertise only summary route 160.1.0.0/16.

```
[SwitchA] ospf
[SwitchA-ospf-1] import-route direct
[SwitchA-ospf-1] asbr-summary 160.1.0.0 16
```

Configure OSPF to redistribute direct routes on Switch B, and configure Switch B to advertise only summary route 160.2.0.0/16.

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route direct
[SwitchB-ospf-1] asbr-summary 160.2.0.0 16
```

Configure OSPF to redistribute routes from BGP on Switch C.

```
[SwitchC] ospf
[SwitchC-ospf-1] import-route bgp
```

Configure OSPF to redistribute routes from BGP on Switch D.

```
[SwitchD] ospf
[SwitchD-ospf-1] import-route bgp
```

Configuration files

- Switch A:

```
#
```

```
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
ospf 1
 asbr-summary 160.1.0.0 255.255.0.0
 import-route direct
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
```

- Switch B:

```
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 asbr-summary 160.2.0.0 255.255.0.0
 import-route direct
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
```

- Switch C:

```
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.1.3.2 255.255.255.0
#
```

```
ospf 1
 import-route bgp
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
#
```

- Switch D:

```
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.4.2 255.255.255.0
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
```

Example: Configuring OSPF to advertise a summary route

Applicable product matrix

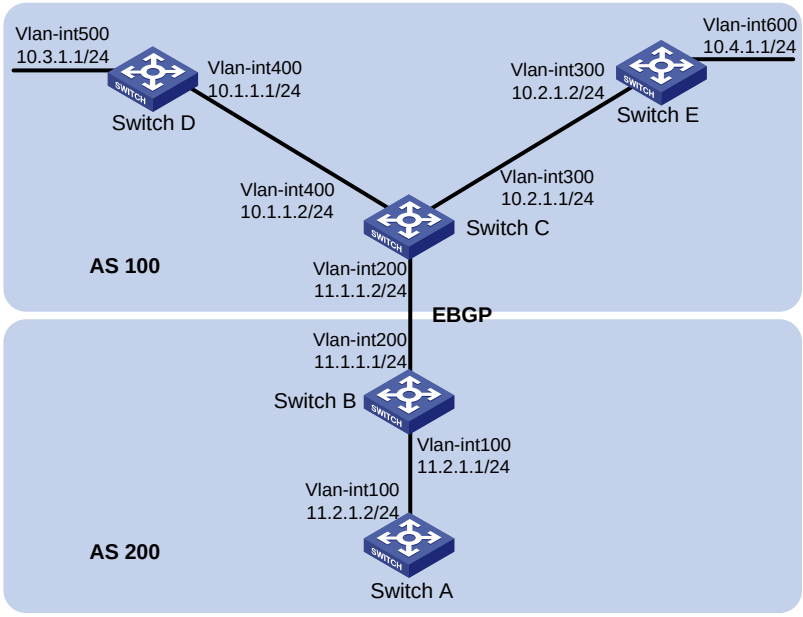
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 161, AS 100 and AS 200 use BGP to exchange routing information, and the switches in AS 100 and AS 200 run OSPF.

Configure route summarization on Switch B to reduce the number of routes advertised to AS 200.

Figure 161 Network diagram



Configuration restrictions and guidelines

When you configure OSPF to advertise a summary route, follow these restrictions and guidelines:

- Use the **asbr-summary** command on an ASBR to do the following:
  - Enable the ASBR to summarize redistributed routes in the specified address range into a single route.
  - Advertise the summary route to neighbors.
- Use the **undo asbr-summary** command to remove the summary route and enable the ASBR to advertise the specific routes.
- Only active OSPF routes that exist in the local OSPF routing table can be redistributed by BGP.

Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 161. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
```

```
[SwitchB-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure Switch D.

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
```

Configure Switch E.

```
<SwitchE> system-view
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

3. Configure an EBGP connection between Switch B and Switch C:

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] peer 11.1.1.2 as-number 100
[SwitchB-bgp] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] bgp 100
[SwitchC-bgp] peer 11.1.1.1 as-number 200
```

4. Configure route redistribution on Switch B and Switch C:

Configure BGP to redistribute OSPF routes on Switch C.

```
[SwitchC-bgp] import-route ospf
```

Configure BGP to redistribute direct routes on Switch C.

```
[SwitchC-bgp] import-route direct
```

Configure OSPF to redistribute routes from BGP on Switch C.

```
[SwitchC] ospf
[SwitchC-ospf-1] import-route bgp
```

Configure BGP to redistribute OSPF routes on Switch B.

```
[SwitchB-bgp] import-route ospf
```

Configure BGP to redistribute direct routes on Switch B.

```
[SwitchB] bgp 200
[SwitchB-bgp] import-route direct
```

Configure OSPF to redistribute routes from BGP on Switch B.

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
```

Display routing information on Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

10.1.1.0/24         O_ASE   150  1            11.2.1.1        Vlan100
10.2.1.0/24         O_ASE   150  1            11.2.1.1        Vlan100
10.3.1.0/24         O_ASE   150  1            11.2.1.1        Vlan100
10.4.1.0/24         O_ASE   150  1            11.2.1.1        Vlan100
11.2.1.0/24         Direct  0    0            11.2.1.2        Vlan100
11.2.1.2/32         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

5. Configure route summarization on Switch B to advertise a summary route 10.0.0.0/8.

```
[SwitchB-ospf-1] asbr-summary 10.0.0.0 8
```

Verifying the configuration

Display routing information on Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

10.0.0.0/8          O_ASE   150  2            11.2.1.1        Vlan100
11.2.1.0/24         Direct  0    0            11.2.1.2        Vlan100
11.2.1.2/32         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

The output shows that the following routes are summarized into a single route 10.0.0.0/8:

- 10.1.1.0/24
- 10.2.1.0/24
- 10.3.1.0/24
- 10.4.1.0/24

Configuration files

- Switch A:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 11.2.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 11.2.1.0 0.0.0.255
#
```

- Switch B:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 11.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 11.1.1.1 255.255.255.0
#
bgp 200
 undo synchronization
 peer 11.1.1.2 as-number 100
 import-route direct
#
ospf 1
 asbr-summary 10.0.0.0 255.0.0.0
 import-route bgp
 area 0.0.0.0
  network 11.2.1.0 0.0.0.255
#
```

- Switch C:

```
#
vlan 200
#
vlan 300
#
vlan 400
#
interface Vlan-interface200
 ip address 11.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface400
```

```
 ip address 10.1.1.2 255.255.255.0
#
bgp 100
 import-route ospf 1
 undo synchronization
 peer 11.1.1.1 as-number 200
 import-route direct
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
import-route bgp
#
```

- Switch D:

```
#
vlan 400
#
vlan 500
#
interface Vlan-interface400
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface500
 ip address 10.3.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
```

- Switch E:

```
#
vlan 300
#
vlan 600
#
interface Vlan-interface300
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface600
 ip address 10.4.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
```

Example: Configuring OSPF DR election

Applicable product matrix

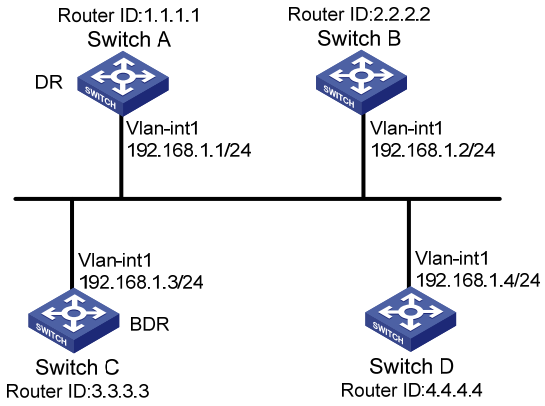
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 162:

- Run OSPF on Switch A, Switch B, Switch C, and Switch D that are on the same network.
- Designate Switch A as the DR, and designate Switch C as the BDR.

Figure 162 Network diagram



Configuration restrictions and guidelines

When you configure OSPF DR election, follow these restrictions and guidelines:

- When a switch with a higher router priority is added to the network after DR and BDR election has taken place, the switch does not become the DR or BDR immediately. Instead, it can become a DR or BDR only at the next DR and BDR election.
- The role of a switch is subnet (or interface) specific. For example, a switch might be a DR on one interface and a BDR or DROther on another interface.

Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 162. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[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> system-view
[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> system-view
[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> system-view
[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
```

Display OSPF neighbor information on Switch A.

```
[SwitchA] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.1(Vlan-interface1)'s neighbors
 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 38  sec
   Neighbor is up for 00:01:31
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
```

```
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 31  sec
  Neighbor is up for 00:01:28
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2

 Router ID: 4.4.4.4          Address: 192.168.1.4      GR State: Normal
  State: Full  Mode: Nbr is Master  Priority: 1
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 31  sec
  Neighbor is up for 00:01:28
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2
```

The output shows that Switch D is the DR and Switch C is the BDR.

3. Configure router priorities on interfaces:

Configure Switch A.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ospf dr-priority 3
[SwitchA-Vlan-interface1] quit
```

Configure Switch C.

```
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface] quit
```

Configure Switch D.

```
[SwitchD] interface vlan-interface 1
[SwitchD-Vlan-interface1] ospf dr-priority 1
[SwitchD-Vlan-interface] quit
```

Configure Switch B.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit
```

Display neighbor information on Switch D.

```
[SwitchD] display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
  State: Full  Mode:Nbr is  Slave  Priority: 3
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 31  sec
  Neighbor is up for 00:11:17
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 3

 Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
```

```
  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
  Neighbor is up for 00:11:19
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 3

 Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
  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
  Neighbor is up for 00:11:15
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 3
```

The output shows that the DR and BDR are not changed, because the priority settings do not take effect immediately.

Verifying the configuration

Restart the OSPF process of Switch D.

```
<SwitchD> reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

Display neighbor information on Switch D.

```
[SwitchD] display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1      GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 3
   DR: 192.168.1.3  BDR: 192.168.1.1  MTU: 0
   Dead timer due in 39  sec
   Neighbor is up for 00:01:40
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 0
   DR: 192.168.1.3  BDR: 192.168.1.1  MTU: 0
   Dead timer due in 35  sec
   Neighbor is up for 00:01:44
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 2
   DR: 192.168.1.3  BDR: 192.168.1.1  MTU: 0
```

```
  Dead timer due in 39  sec
  Neighbor is up for 00:01:41
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2
```

The output shows that Switch C becomes the DR, and Switch A becomes the BDR.

Restart the OSPF process of Switch C.

```
<SwitchC> reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

Display neighbor information on Switch D.

```
[SwitchD] display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1      GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 3
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 39  sec
   Neighbor is up for 00:01:40
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 0
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35  sec
   Neighbor is up for 00:01:44
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 2
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 39  sec
   Neighbor is up for 00:01:41
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2
```

The output shows that Switch A becomes the DR, and Switch C becomes the BDR.

A neighbor state of **Full** indicates Switch D has established an adjacency with the neighbor. If the neighbor state is **2-way**, the two switches are not the DR or the BDR, and they do not exchange LSAs.

Display OSPF interface information on Switch A.

```
[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
```

The interface state **DROther** means the interface is not the DR or BDR.

Configuration files

- Switch A:

```
#
 router id 1.1.1.1
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
 ospf dr-priority 3
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
```

- Switch B:

```
#
 router id 2.2.2.2
#
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
 ospf dr-priority 0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
```

- Switch C:

```
#
 router id 3.3.3.3
#
interface Vlan-interface1
 ip address 192.168.1.3 255.255.255.0
```

```
 ospf dr-priority 2
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
```

- Switch D:

```
#
 router id 4.4.4.4
#
interface Vlan-interface1
 ip address 192.168.1.4 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
```

Example: Configuring an OSPF virtual link

Applicable product matrix

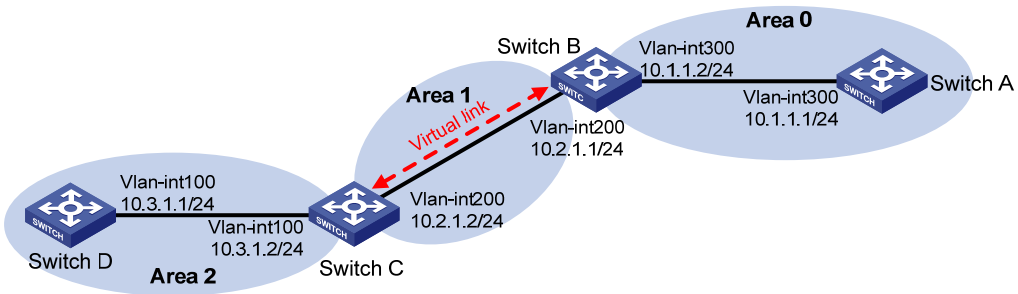
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 163, Area 2 and Area 0 are not directly connected, and switches in Area 2 cannot reach switches in other areas.

Configure a virtual link between Switch B and Switch C through Area 1 to connect the whole network so that all switches can reach each other.

Figure 163 Network diagram



Configuration restrictions and guidelines

When you configure an OSPF virtual link, follow these restrictions and guidelines:

- Configure the **vlink-peer** command on both ends of a virtual link. The **hello** and **dead** intervals must be identical on both ends of the virtual link.
- Make sure you use the correct neighbor router ID when you configure a virtual link by using the **vlink-peer** command. The ID might not be the IP address of the neighbor interface.
- Virtual links are not allowed in stub areas or NSSA areas.

Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 163. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf 1 router-id 1.1.1.1
[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] quit
```

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[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] quit
[SwitchB-ospf-1] area 1
[SwitchB–ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchB–ospf-1-area-0.0.0.1] quit
```

   # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC–ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchC–ospf-1-area-0.0.0.2] quit
```

   # Configure Switch D.

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
```

   # Display OSPF routing information on Switch B.

```
[SwitchB] display ospf routing
          OSPF Process 1 with Router ID 2.2.2.2
```

```
                  Routing Tables
 Routing for Network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        2        Transit 10.2.1.1        3.3.3.3         0.0.0.1
 10.1.1.0/24        2        Transit 10.1.1.2        2.2.2.2         0.0.0.0
 Total Nets: 2
 Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

The output shows that the routing table of Switch B has no route to Area 2 when Area 0 has no direct connection to Area 2.

3. Configure a virtual link:

   # Configure Switch B.

```
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

   # Configure Switch C.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1-area-0.0.0.1] quit
```

Verifying the configuration

Display OSPF routing information on Switch B.

```
[SwitchB] display ospf routing
          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Tables
 Routing for Network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        2        Transit 10.2.1.1        3.3.3.3         0.0.0.1
 10.3.1.0/24        5        Inter   10.2.1.2        3.3.3.3         0.0.0.0
 10.1.1.0/24        2        Transit 10.1.1.2        2.2.2.2         0.0.0.0
 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

The output shows that Switch B has learned the route 10.3.1.0/24 to Area 2.

Configuration files

- Switch A:

```
#
vlan 300
#
interface Vlan-interface300
 ip address 10.1.1.1 255.255.255.0
#
ospf 1 router-id 1.1.1.1
```

```
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 10.1.1.2 255.255.255.0
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.1
  network 10.2.1.0 0.0.0.255
  vlink-peer 3.3.3.3
#
```

- Switch C:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.3.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.1
  network 10.2.1.0 0.0.0.255
  vlink-peer 2.2.2.2
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#
```

- Switch D:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.3.1.1 255.255.255.0
#
```

```
ospf 1 router-id 4.4.4.4
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#
```

Example: Configuring OSPF GR

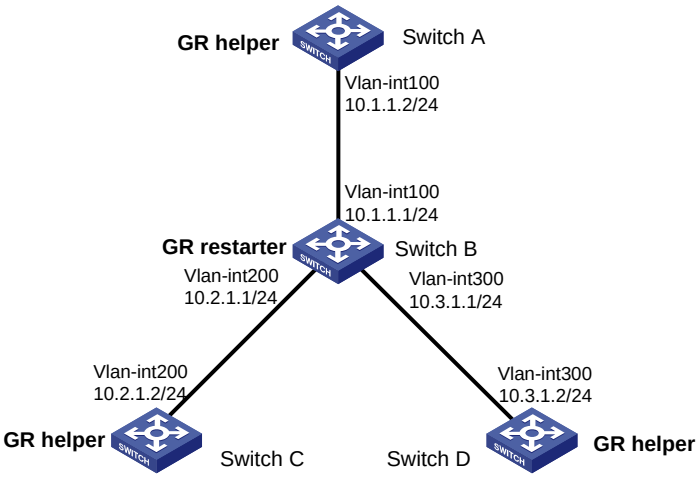
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 164, configure IETF Graceful Restart (GR) so that route flapping, route changes, or forwarding interruption does not occur during an active/standby switchover or a routing protocol restart on Switch B.

Figure 164 Network diagram



Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 164. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[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] return
```

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf 1
[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 10.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] return
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] return
```

Configure Switch D.

```
<SwitchD> system-view
[SwitchD] ospf 1
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] return
```

3. Configure OSPF GR:

Configure Switch B as the IETF OSPF GR restarter.

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] opaque-capability enable
[SwitchB-ospf-1] graceful-restart ietf
```

Configure Switch A as the GR helper.

```
<SwitchA> system-view
[SwitchA] ospf 1
[SwitchA-ospf-1] opaque-capability enable
```

Configure Switch C as the GR helper.

```
<SwitchC> system-view
[SwitchC] ospf 1
[SwitchC-ospf-1] opaque-capability enable
```

Configure Switch D as the GR helper.

```
<SwitchD> system-view
[SwitchD] ospf 1
[SwitchD-ospf-1] opaque-capability enable
```

Verifying the configuration

Restart the OSPF process on Switch B to trigger GR. During the GR process, verify the following items:

- No changes are made to the switch routing tables.
- No network interruption occurs (by using the **ping** command).

Configuration files

- Switch A:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
ospf 1
 opaque-capability enable
area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.3.1.2 255.255.255.0
#
ospf 1
 opaque-capability enable
 graceful-restart ietf
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
```

- Switch C:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.2.1.2 255.255.255.0
#
ospf 1
```

```
 opaque-capability enable
area 0.0.0.0
  network 10.2.1.0 0.0.0.255
#
```

- Switch D:

```
#
vlan 300
#
interface Vlan-interface300
 ip address 10.3.1.2 255.255.255.0
#
ospf 1
 opaque-capability enable
area 0.0.0.0
  network 10.3.1.0 0.0.0.255
#
```

Example: Configuring BFD for OSPF

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 165, Switch A, Switch B, and Switch C run OSPF between them.

Configure OSPF BFD on Switch A and Switch B to meet the following requirements:

- Switch A and Switch B can quickly detect the failure of the link over the Layer 2 switch, and notify OSPF of the failure.
- Switch A and Switch B communicate through Switch C when the link over the Layer 2 switch fails.

Figure 165 Network diagram

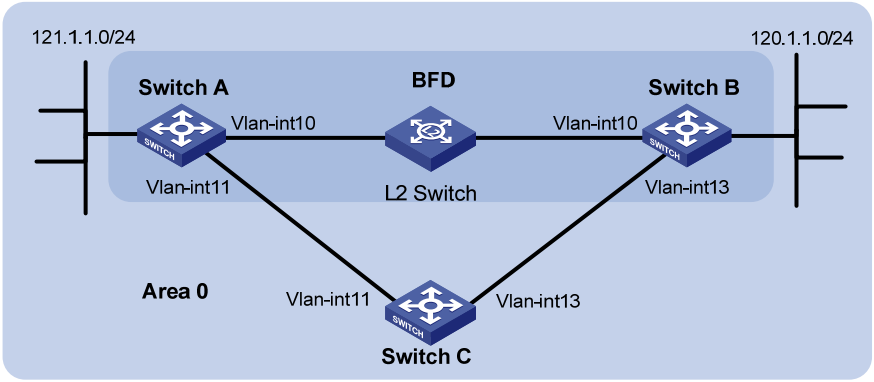


Table 16 IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int10	10.1.0.102/24	Switch B	Vlan-int10	10.1.0.100/24
	Vlan-int11	11.1.1.1/24		Vlan-int13	13.1.1.1/24
Switch C	Vlan-int11	11.1.1.2/24			
	Vlan-int13	13.1.1.2/24			

Configuration restrictions and guidelines

When you configure BFD for OSPF, follow these restrictions and guidelines:

- This example uses the bidirectional control detection. BFD detection requires BFD configuration on both OSPF switches on the link.
- Both ends of a BFD session must be on the same network segment and in the same OSPF area.

Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 165. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 121.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
[SwitchA] interface vlan 11
[SwitchA-Vlan-interface11] ospf cost 2
[SwitchA-Vlan-interface11] quit
```

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 120.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
[SwitchB] interface vlan-interface 13
[SwitchB-Vlan-interface13] ospf cost 2
[SwitchB-Vlan-interface13] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

3. Enable BFD:

Configure Switch A.

```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ospf bfd enable
[SwitchA-Vlan-interface10] quit
[SwitchA] quit
```

Configure Switch B.

```
[SwitchB] bfd session init-mode active
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ospf bfd enable
```

Verifying the configuration

Display BFD information on Switch A.

```
<SwitchA> display bfd session
 Total Session Num: 1            Init Mode: Active
 Session Working Under Ctrl Mode:
 LD/RD         SourceAddr      DestAddr        State Holdtime Interface
 3/1           10.1.0.102      10.1.0.100      Up    1700ms   vlan10
```

Display routes destined for 120.1.1.0/24 on Switch A.

```
<SwitchA> display ip routing-table 120.1.1.0 verbose
Routing Table : Public
Summary Count : 1
  Destination: 120.1.1.0/24
     Protocol: OSPF            Process ID: 0
   Preference: 0                     Cost: 2
 IpPrecedence:                   QosLcId:
```

```
     NextHop: 10.1.0.100    Interface: Vlan-interface10
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active Adv            Age: 00h58m10s
          Tag: 0
```

The output shows that Switch A communicates with Switch B through VLAN-interface 10.

On the Layer 2 switch, shut down the interface that connects VLAN-interface 10 of Switch A, and then display BFD information on Switch A.

```
<SwitchA> display bfd session
```

The output shows that the BFD session between Switch A and Switch B is removed.

Display routes destined for 120.1.1.0/24 on Switch A.

```
<SwitchA> display ip routing-table 120.1.1.0 verbose
Routing Table : Public
Summary Count : 1
  Destination: 120.1.1.0/24
     Protocol: OSPF            Process ID: 1
   Preference: 10                    Cost: 4
 IpPrecedence:                    QosLcId:
     NextHop: 11.1.1.2       Interface: Vlan-interface11
    BkNextHop: 0.0.0.0        BkInterface:
  RelyNextHop: 0.0.0.0          Neighbor : 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
  BKTunnel ID: 0x0                BKLabel: NULL
        State: Active Adv            Age: 00h58m10s
          Tag: 0
```

The output shows that Switch A communicates with Switch B through VLAN-interface 11.

Configuration files

- Switch A:

```
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
 ospf bfd enable
#
vlan 11
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
vlan 12
#
```

```
interface Vlan-interface12
 ip address 121.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
network 11.1.1.0 0.0.0.255
network 121.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.0.100 255.255.255.0
 ospf bfd enable
#
vlan 12
#
interface Vlan-interface12
 ip address 120.1.1.1 255.255.255.0
#
vlan 13
#
interface Vlan-interface13
 ip address 13.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
network 13.1.1.0 0.0.0.255
network 120.1.1.0 0.0.0.255
#
```

- Switch C:

```
#
vlan 11
#
interface Vlan-interface11
 ip address 11.1.1.2 255.255.255.0
#
vlan 13
#
interface Vlan-interface13
 ip address 13.1.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 11.1.1.0 0.0.0.255
```

```
network 13.1.1.0 0.0.0.255
#
```

PIM configuration examples

This chapter provides PIM configuration examples.

Based on the implementation mechanism, PIM includes the following categories:

- **Protocol Independent Multicast–Dense Mode**—PIM-DM uses the ASM model and is suitable for small-sized networks with densely distributed multicast members.
- **Protocol Independent Multicast–Sparse Mode**—PIM-SM uses the ASM model and is suitable for large- and medium-sized networks with sparsely and widely distributed multicast members. For refined management, PIM-SM employs the administrative scoping mechanism to provide services for private group addresses in specific admin-scoped zones.
- **Protocol Independent Multicast Source-Specific Multicast**—PIM-SSM provides a solution for source-specific multicast.

General configuration restrictions and guidelines

When you configure PIM, follow these restrictions and guidelines:

- All the interfaces on a switch must operate in the same PIM mode.
- If a VLAN is running a Layer 2 multicast protocol, do not configure Layer 3 multicast protocols on the VLAN interface of this VLAN.

Example: Configuring PIM-DM

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 166:

- All the switches are Layer 3 switches, and they run OSPF.
- The multicast source, receiver hosts, and switches can communicate with each other through unicast routes.

Configure PIM-DM on each switch, so that multicast data can be sent to receivers in **N1** and **N2**.

Figure 166 Network diagram

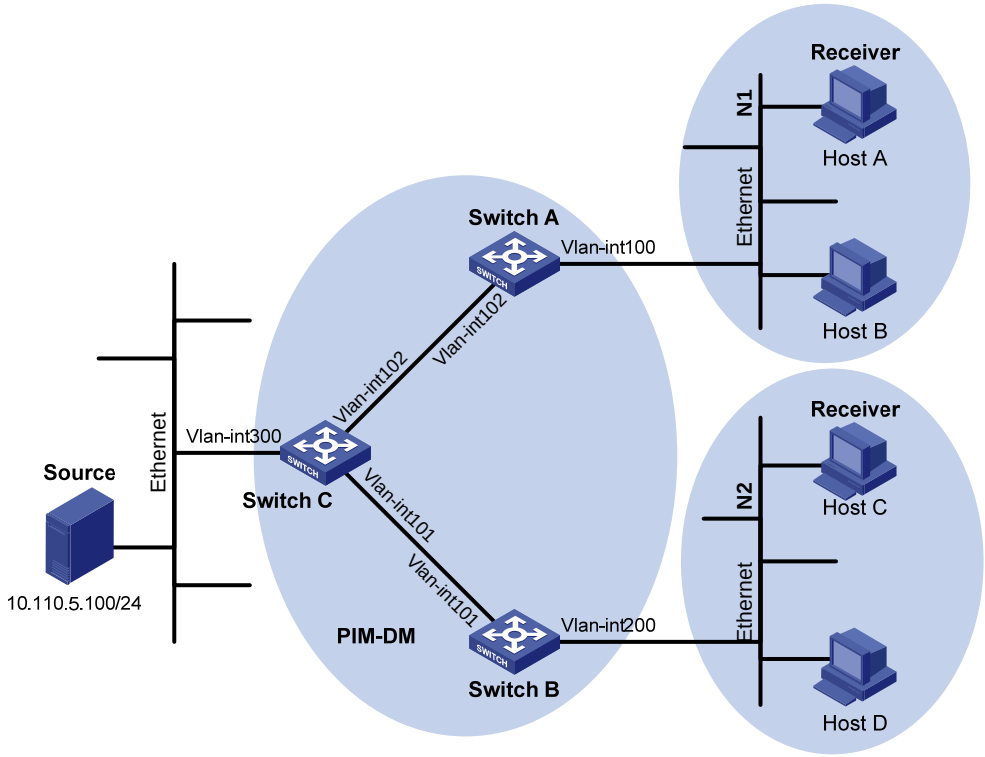


Table 17 IP address assignment

Device	Interface	IP address
Switch A	VLAN-interface 100	10.110.1.1/24
Switch A	VLAN-interface 102	192.168.1.1/24
Switch B	VLAN-interface 200	10.110.2.1/24
Switch B	VLAN-interface 101	192.168.2.1/24
Switch C	VLAN-interface 300	10.110.5.1/24
Switch C	VLAN-interface 102	192.168.1.2/24
Switch C	VLAN-interface 101	192.168.2.2/24

Configuration restrictions and guidelines

When you configure PIM-DM, enable IGMP on the edge switches to establish and maintain multicast group membership at Layer 3.

Configuration procedures

1. Assign an IP address to each interface according to Table 17. (Details not shown.)
2. Configure OSPF on the switches in the PIM-DM domain. (Details not shown.)
3. Enable IP multicast routing and PIM-DM:

   # On Switch A, enable IP multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
```

On Switch A, enable PIM-DM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
```

On Switch B and Switch C, enable IP multicast routing and PIM-DM in the same way Switch A is configured. (Details not shown.)

4. Enable IGMPv2 on the interfaces that are directly connected to user networks:

On Switch A, enable IGMP on VLAN-interface 100. (By default, the IGMP version is 2.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

On Switch B, enable IGMP on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

To verify that correct multicast group entries can be created on the switches:

1. Send IGMPv2 reports from Host A and Host C to join the multicast group **225.1.1.1**.
2. Send multicast data from the multicast source **10.110.5.100/24** to the multicast group.
3. Use the **display pim routing-table** command to display PIM routing table information on each switch:

Display the PIM routing table on Switch C.

```
[SwitchC] 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: 00:03:27
     Upstream interface: Vlan-interface300
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: Vlan-interface101
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
         2: Vlan-interface102
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

Display the PIM routing table on Switch A.

```
[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: 00:04:25
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface100
                  Protocol: igmp, UpTime: 00:04:25, Expires: never

 (10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:06:14
     Upstream interface: Vlan-interface102,
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface100
                  Protocol: pim-dm, UpTime: 00:04:25, Expires: never
```

The output on Switch B is similar.

The output shows the following:

- An SPT has been established through traffic flooding. Switches on the SPT path (Switch A and Switch B) have their (S, G) entries.
- Because Host A sends an IGMP report to Switch A to join the multicast group G, a (*, G) entry is generated on Switch A.

Configuration files

- Switch A:

```
#
 multicast routing-enable
#
vlan 100
#
vlan 102
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0.
 igmp enable
 pim dm
#
interface Vlan-interface102
 ip address 192.168.1.1 255.255.255.0
```

```
 pim dm
#
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
#
```

- Switch B:

```
#
 multicast routing-enable
#
vlan 101
#
vlan 200
#
interface Vlan-interface101
 ip address 192.168.2.1 255.255.255.0.
 pim dm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 pim dm
#
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
#
```

- Switch C:

```
#
 multicast routing-enable
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
 ip address 192.168.2.2 255.255.255.0.
 pim dm
#
interface Vlan-interface102
 ip address 192.168.1.2 255.255.255.0
 pim dm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim dm
```

```
#
ospf 1
 area 0.0.0.0
  network 10.110.5.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
```

Example: Configuring PIM-SM

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 167:

- All the switches are Layer 3 switches, and they run OSPF.
- The multicast source, receiver hosts, and switches can communicate with each other through unicast routes.

Configure PIM-SM on each switch, so that multicast data of the multicast groups in the range of **225.1.1.0/24** can be sent to receivers in **N1** and **N2**.

Figure 167 Network diagram

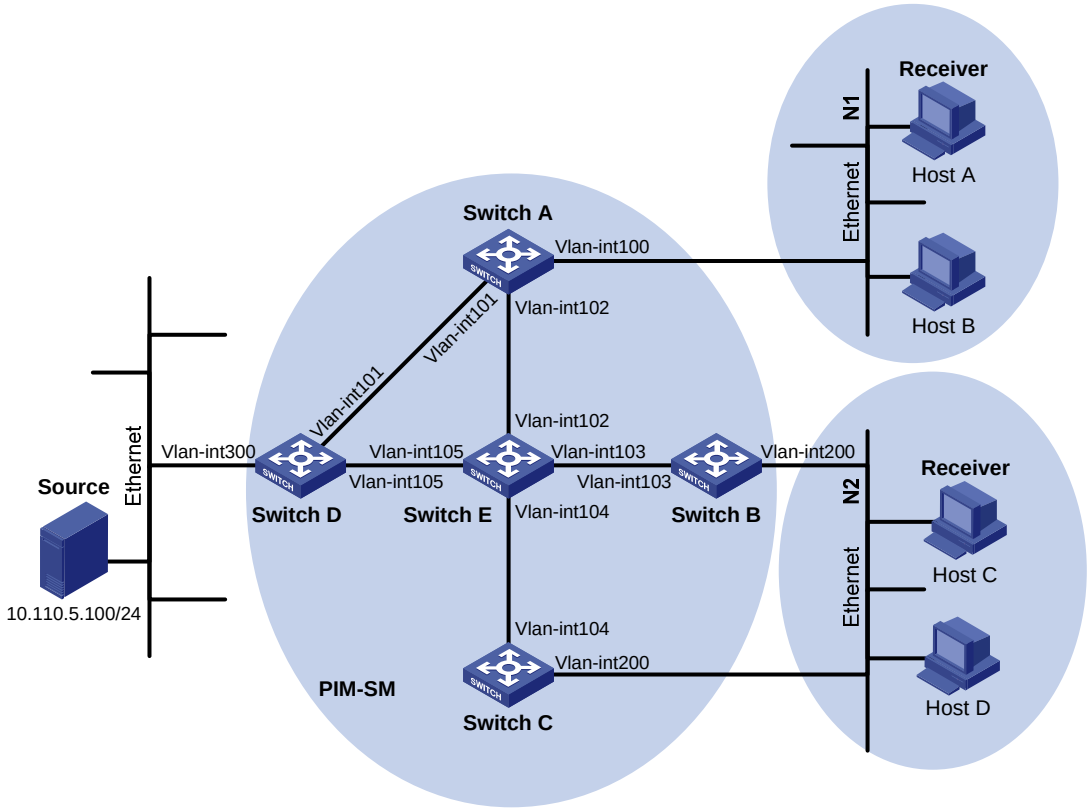


Table 18 IP address assignment

Device	Interface	IP address
Switch A	VLAN-interface 100	10.110.1.1/24
Switch A	VLAN-interface 101	192.168.1.1/24
Switch A	VLAN-interface 102	192.168.9.1/24
Switch B	VLAN-interface 200	10.110.2.1/24
Switch B	VLAN-interface 103	192.168.2.1/24
Switch C	VLAN-interface 200	10.110.2.2/24
Switch C	VLAN-interface 104	192.168.3.1/24
Switch D	VLAN-interface 300	10.110.5.1/24
Switch D	VLAN-interface 101	192.168.1.2/24
Switch D	VLAN-interface 105	192.168.4.2/24
Switch E	VLAN-interface 104	192.168.3.2/24
Switch E	VLAN-interface 103	192.168.2.2/24
Switch E	VLAN-interface 102	192.168.9.2/24
Switch E	VLAN-interface 105	192.168.4.1/24

Requirements analysis

Because receivers request multicast data of the multicast groups in the range of **225.1.1.0/24**, you must configure C-RPs to provide services for this group range.

To lessen the burden on a single RP, configure multiple C-RPs on the network. For example, configure Switch D and Switch E as C-RPs so they can provide services for different multicast groups through the bootstrap mechanism.

To avoid communication interruption caused by a single-point failure of the BSR, configure multiple C-BSRs on the network. For example, you can configure a C-BSR on a switch that acts as a C-RP. When the BSR fails, other C-BSRs can elect a new BSR.

Configuration restrictions and guidelines

When you configure PIM-SM, follow these restrictions and guidelines:

- If multiple Layer 3 switches are connected to a shared-media network, configure IGMP and PIM-SM on each Layer 3 switch. When one switch fails, other switches can be used for multicast forwarding.
- HP recommends that you configure C-BSRs and C-RPs on Layer 3 switches on the backbone network.
- If you do not specify the multicast group range to which a C-RP is designated, the C-RP provides services for all multicast groups.

Configuration procedures

1. Assign an IP address and subnet mask to each interface according to Table 18. (Details not shown.)
2. Configure OSPF on all switches on the PIM-SM network. (Details not shown.)
3. Enable IP multicast routing and PIM-SM:

   # On Switch A, enable IP multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing-enable
   ```

   # On Switch A, enable PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] pim sm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim sm
   [SwitchA-Vlan-interface101] quit
   [SwitchA] interface vlan-interface 102
   [SwitchA-Vlan-interface102] pim sm
   [SwitchA-Vlan-interface102] quit
   ```

   # On Switch B, Switch C, Switch D, and Switch E, enable IP multicast routing and PIM-SM in the same way Switch A is configured. (Details not shown.)
4. Enable IGMPv2 on the interfaces that are directly connected to stub networks:

   # On Switch A, enable IGMP on VLAN-interface 100. (By default, the IGMP version is 2.)

   ```
   [SwitchA] interface vlan-interface 100
   ```

```
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

On Switch B and Switch C, enable IGMP on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

5. Configure C-BSRs and C-RPs:

On Switch D, create an ACL to define a multicast group range to which the C-RP is designated.

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
```

On Switch D, configure VLAN-interface 105 as a C-RP, referencing ACL 2005 to provide services for only the multicast groups in the range of **225.1.1.0/24**.

```
[SwitchD] pim
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005
```

On Switch D, configure VLAN-interface 105 as a C-BSR. Set its hash mask length and priority to 32 and 10, respectively.

```
[SwitchD-pim] c-bsr vlan-interface 105 32 10
[SwitchD-pim] quit
```

On Switch E, create an ACL to define a multicast group range to which C-RP is designated.

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
```

On Switch E, configure VLAN-interface 105 as a C-RP. Reference ACL 2005 to provide services only for the multicast groups in the range of **225.1.1.0/24**.

```
[SwitchE] pim
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
```

On Switch E, configure VLAN-interface 102 as a C-BSR. Set its hash mask length and priority to 32 and 20, respectively.

```
[SwitchE-pim] c-bsr vlan-interface 102 32 20
[SwitchE-pim] quit
```

Verifying the configuration

1. Verify that the IGMP querier and the DR are correctly elected on the shared-media network **N2**:

Display information about the IGMP querier election on Switch B.

```
[SwitchB] display igmp interface
Interface information of VPN-Instance: public net
 Vlan-interface200(10.110.2.1):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Querier for IGMP: 10.110.2.1 (this router)
  Total 1 IGMP Group reported
```

Display information about the IGMP querier election on Switch C.

```
[SwitchC] display igmp interface
Interface information of VPN-Instance: public net
 Vlan-interface200(10.110.2.2):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Querier for IGMP: 10.110.2.1
  Total 1 IGMP Group reported
```

The output shows that Switch B is elected the IGMP querier. (The switch with a lower IP address wins the IGMP querier election.)

Display PIM information on Switch B.

```
[SwitchB] display pim interface
 VPN-Instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan103             1      30         1          192.168.2.2
 Vlan200             1      30         1          10.110.2.2
```

Display PIM information on Switch C.

```
[SwitchC] display pim interface
 VPN-Instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan104             1      30         1          192.168.3.2
 Vlan200             1      30         1          10.110.2.2      (local)
```

The output shows that Switch C is elected the DR. (The switch that has a higher IP address wins the DR election if the two switches have the same DR priority. The DR priority is identified by the DR priority field in hello packets.)

2. Verify that correct multicast group entries can be created on the switches:
   a. Send an IGMPv2 report from Host A to join the multicast group **225.1.1.1**.
   b. Send multicast data from the multicast source **10.110.5.100** to the multicast group.
   c. Use the **display pim routing-table** command to display PIM routing table information on the switches:

      # Display the PIM routing table on Switch A.

```
[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: Vlan-interface102,
         Upstream neighbor: 192.168.9.2
         RPF prime neighbor: 192.168.9.2
     Downstream interface(s) information:
       Total number of downstreams: 1
```

```
            1: Vlan-interface100
                   Protocol: igmp, UpTime: 00:13:46, Expires:00:03:06

 (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: Vlan-interface101,
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface100
                  Protocol: pim-sm, UpTime: 00:00:42, Expires:00:03:06
```

The output on Switch B and Switch C is similar to that on Switch A.

Display the PIM routing table on Switch D.

```
[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)
     RP: 192.168.9.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:00:42
     Upstream interface: Vlan-interface300
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface101
                  Protocol: pim-sm, UpTime: 00:00:42, Expires:00:02:06
```

Display the PIM routing table on Switch E.

```
[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: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface102
                  Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22
```

```
(10.110.5.100, 225.1.1.1)
    RP: 192.168.9.2 (local)
    Protocol: pim-sm, Flag: RPT SPT ACT
    UpTime: 00:25:32
    Upstream interface: Vlan-interface105
        Upstream neighbor: 192.168.4.2
        RPF prime neighbor: 192.168.4.2
    Downstream interface(s) information: None
```

The output shows the following:

- The RP for the multicast group **225.1.1.1** is Switch E, based on the hash calculation.
- An SPT has been built between the source-side DR (Switch D) and the RP (Switch E).
- An RPT has been built between the receiver-side DR (Switch A) and the RP (Switch E), and Switch A and Switch E have created (*, G) entries. After receiving multicast data, the receiver-side DR (Switch A) immediately switches from the RPT to the SPT. A new SPT is built between the receiver-side DR (Switch A) and the source-side DR (Switch D). The switches (Switch A and Switch D) on the new SPT path have their (S, G) entries.

Configuration files

- Switch A:

```
#
multicast routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 192.168.9.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.9.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
#
```

- Switch B:

```
#
multicast routing-enable
```

```
#
vlan 103
#
vlan 200
#
interface Vlan-interface103
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 pim sm
#
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
#
```

- Switch C:

```
#
multicast routing-enable
#
vlan 104
#
vlan 200
#
interface Vlan-interface104
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.2 255.255.255.0
 igmp enable
 pim sm
#
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
#
```

- Switch D:

```
#
multicast routing-enable
#
acl number 2005
 rule 0 permit source 225.1.1.0 0.0.0.255
#
```

```
vlan 101
#
vlan 105
#
vlan 300
#
interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
#
Pim
 c-bsr hash-length 32
 c-bsr priority 10
 c-bsr Vlan-interface105
 c-rp Vlan-interface105 group-policy 2005
#
```

- Switch E:

```
#
multicast routing-enable
#
acl number 2005
 rule 0 permit source 225.1.1.0 0.0.0.255
#
vlan 102 to 104
#
vlan 105
#
interface Vlan-interface102
 ip address 192.168.9.2 255.255.255.0
 pim sm
#
interface Vlan-interface103
 ip address 192.168.2.2 255.255.255.0
 pim sm
```

```
#
interface Vlan-interface104
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.9.0 0.0.0.255
  network 192.168.2.0 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 hash-length 32
 c-bsr priority 20
 c-bsr Vlan-interface102
 c-rp Vlan-interface102 group-policy 2005
#
```

Example: Configuring PIM-SM admin-scoped zones

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 168:

- All switches are Layer 3 switches, and they run OSPF.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.

Use the PIM-SM administrative scoping mechanism to achieve the following purposes:

- Divide the whole network into admin-scoped zone 1, admin-scoped zone 2, and the global-scoped zone.
- Each admin-scoped zone provides services for the multicast groups in the range of **239.0.0.0/8**. **Source 1** in admin-scoped zone 1. **Source 2** in admin-scoped zone 2 sends multicast data only to

multicast groups in this range. Receivers in each admin-scoped zone can request multicast data only within the local zone.

- **Source 3** in the global-scoped zone sends multicast data to all multicast groups that are not in the range of **239.0.0.0/8**. All receivers on the network can request multicast data of these multicast groups.

Figure 168 Network diagram

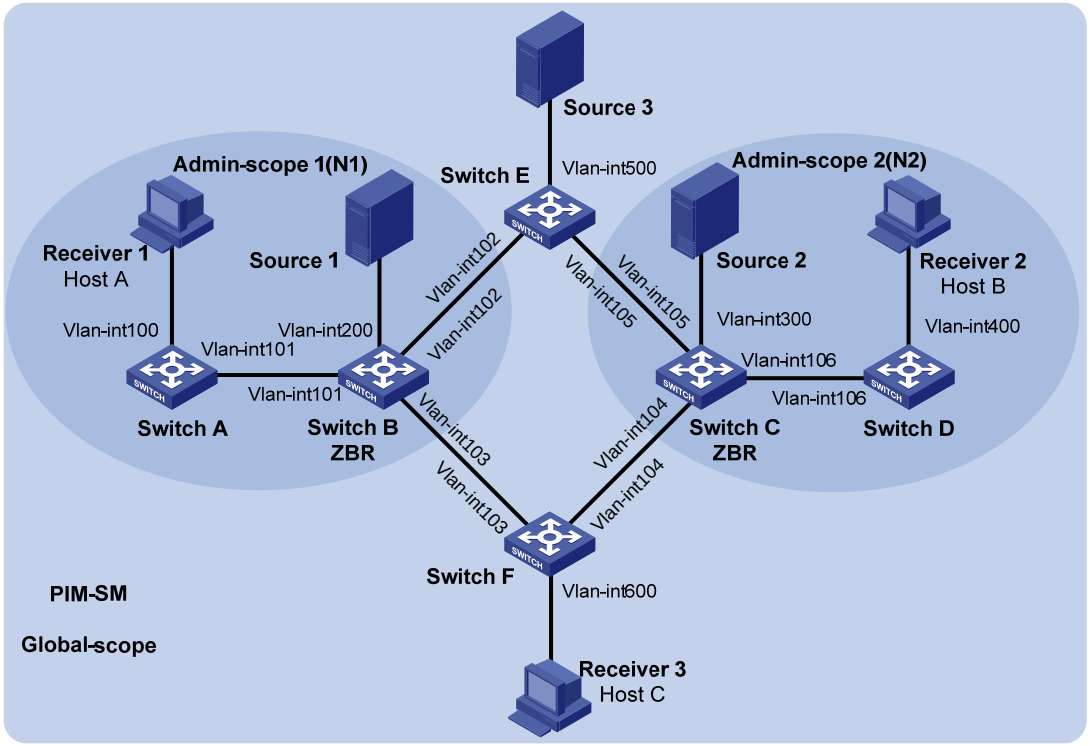


Table 19 IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	VLAN-interface 100	192.168.1.1/24	Switch D	VLAN-interface 106	10.110.6.2/24
Switch A	VLAN-interface 101	10.110.1.1/24	Switch E	VLAN-interface 500	192.168.5.1/24
Switch B	VLAN-interface 200	192.168.2.1/24	Switch E	VLAN-interface 102	10.110.2.2/24
Switch B	VLAN-interface 101	10.110.1.2/24	Switch E	VLAN-interface 105	10.110.5.2/24
Switch B	VLAN-interface 102	10.110.2.1/24	Switch F	VLAN-interface 600	192.168.6.1/24
Switch B	VLAN-interface 103	10.110.3.1/24	Switch F	VLAN-interface 103	10.110.3.2/24
Switch C	VLAN-interface 300	192.168.3.1/24	Switch F	VLAN-interface 104	10.110.4.2/24
Switch C	VLAN-interface 104	10.110.4.1/24	Source 1	N/A	192.168.2.10/24
Switch C	VLAN-interface 105	10.110.5.1/24	Source 2	N/A	192.168.3.10/24
Switch C	VLAN-interface 106	10.110.6.1/24	Source 3	N/A	192.168.5.10/24
Switch D	VLAN-interface 400	192.168.4.1/24			

Requirements analysis

Based on the division of admin-scoped zones and the multicast group range to which each zone is designated, configure the boundaries of each admin-scoped zone on the interfaces through which it connects other zones.

To use the admin-scoped zones and the global-scoped zone to provide services for specific multicast groups, configure C-BSRs and C-RPs in each zone as follows:

- The C-BSRs and C-RPs in each admin-scoped zone provide services for the multicast groups to which the admin-scoped zone is designated.
- The C-BSRs and C-RPs in the global-scoped zone provide services for all multicast groups except multicast groups to which admin-scoped zones are designated.

Configuration restrictions and guidelines

When you configure PIM-SM admin-scoped zones, follow these restrictions and guidelines:

- To establish and maintain multicast group membership at Layer 3, enable IGMP on the interfaces of switches that are directly connected to receiver hosts.
- Before you configure admin-scoped zones, enable administrative scoping on all Layer 3 switches in the PIM-SM domain.
- When you use the **multicast boundary** command to specify the multicast groups to which the admin-scoped zone is designated, the specified multicast group must be in the range of **239.0.0.0/8**.
- The multicast groups to which the C-BSR and the C-RP in each admin-scoped zone are designated must be in the range of **239.0.0.0/8**.

Configuration procedures

1. Assign an IP address and subnet mask to each interface according to Table 19. (Details not shown.)
2. Configure OSPF on all the switches on the PIM-SM network. (Details not shown.)
3. Enable IP multicast routing, administrative scoping, IGMP, and PIM-SM:

   # On Switch A, enable IP multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing-enable
   ```

   # On Switch A, enable administrative scoping.

   ```
   [SwitchA] pim
   [SwitchA-pim] c-bsr admin-scope
   [SwitchA-pim] quit
   ```

   # On Switch A, enable PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] pim sm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim sm
   [SwitchA-Vlan-interface101] quit
   ```

On Switch B, Switch C, Switch D, Switch E, and Switch F, enable IP multicast routing, administrative scoping, and PIM-SM in the same way Switch A is configured. (Details not shown.)

On Switch A, enable IGMP on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface101] quit
```

On Switch D and Switch F, enable IGMP in the same way Switch A is configured. (Details not shown.)

4. Configure admin-scoped zone boundaries:

On Switch B, configure VLAN-interface 102 and VLAN-interface 103 as the boundaries of admin-scoped zone 1.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface103] quit
```

On Switch C, configure VLAN-interface 104 and VLAN-interface 105 as the boundaries of admin-scoped zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 105
[SwitchC-Vlan-interface105] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface105] quit
```

5. Configure C-BSRs and C-RPs:

On Switch B, create an ACL to define a multicast group range to which the C-RP is designated. .

```
[SwitchB] acl number 2001
[SwitchB-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchB-acl-basic-2001] quit
```

On Switch B, configure VLAN-interface 101 as a C-RP, referencing ACL 2001 to provide services for only the multicast groups in the range of **239.0.0.0/8**.

```
[SwitchB] pim
[SwitchB-pim] c-rp vlan-interface 101 group-policy 2001
```

On Switch B, configure VLAN-interface 101 as a C-BSR for admin-scoped zone 1.

```
[SwitchB-pim] c-bsr group 239.0.0.0 8
[SwitchB-pim] c-bsr vlan-interface 101
[SwitchB-pim] quit
```

On Switch C, create an ACL to define a multicast group range to which the C-RP is designated.

```
[SwitchC] acl number 2001
[SwitchC-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchC-acl-basic-2001] quit
```

On Switch C, configure VLAN-interface 106 as a C-RP. Reference ACL 2001 to provide services for only the multicast groups in the range of **239.0.0.0/8**.

```
[SwitchC] pim
```

```
[SwitchC-pim] c-rp vlan-interface 106 group-policy 2001
```

On Switch C, configure VLAN-interface 106 as a C-BSR for admin-scoped zone 2.

```
[SwitchC-pim] c-bsr group 239.0.0.0 8
[SwitchC-pim] c-bsr vlan-interface 106
[SwitchC-pim] quit
```

On Switch E, configure VLAN-interface 102 as a C-BSR and a C-RP for the global-scoped zone.

```
<SwitchE> system-view
[SwitchE] pim
[SwitchE-pim] c-bsr global
[SwitchE-pim] c-bsr vlan-interface 102
[SwitchE-pim] c-rp vlan-interface 102
[SwitchE-pim] quit
```

Verifying the configuration

1. Verify that the BSR has been elected and that the local C-RP configuration in each zone has taken effect:

Display information about the BSR and the locally configured C-RP on Switch B.

```
[SwitchB] display pim bsr-info
 VPN-Instance: public net
 Elected BSR Address: 10.110.2.2
     Priority: 64
     Hash mask length: 30
     State: Accept Preferred
     Scope: Global
     Uptime: 00:01:45
     Expires: 00:01:25
 Elected BSR Address: 10.110.1.2
     Priority: 64
     Hash mask length: 30
     State: Elected
     Scope: 239.0.0.0/8
     Uptime: 00:04:54
     Next BSR message scheduled at: 00:00:06
 Candidate BSR Address: 10.110.1.2
     Priority: 64
     Hash mask length: 30
     State: Elected
     Scope: 239.0.0.0/8

 Candidate RP: 10.110.1.2(Vlan-interface101)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:15
```

Display information about the BSR and the locally configured C-RP on Switch C.

```
[SwitchC] display pim bsr-info
```

```
 VPN-Instance: public net
 Elected BSR Address: 10.110.2.2
     Priority: 64
     Hash mask length: 30
     State: Accept Preferred
     Scope: Global
     Uptime: 00:01:45
     Expires: 00:01:25
 Elected BSR Address: 10.110.6.1
     Priority: 64
     Hash mask length: 30
     State: Elected
     Scope: 239.0.0.0/8
     Uptime: 00:03:48
     Next BSR message scheduled at: 00:01:12
 Candidate BSR Address: 10.110.6.1
     Priority: 64
     Hash mask length: 30
     State: Elected
     Scope: 239.0.0.0/8

 Candidate RP: 10.110.6.1(Vlan-interface106)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:10
```

Display information about the BSR and the locally configured C-RP on Switch E.

```
[SwitchE] display pim bsr-info
 VPN-Instance: public net
 Elected BSR Address: 10.110.2.2
     Priority: 64
     Hash mask length: 30
     State: Elected
     Scope: Global
     Uptime: 00:11:11
     Next BSR message scheduled at: 00:00:49
 Candidate BSR Address: 10.110.2.2
     Priority: 64
     Hash mask length: 30
     State: Elected
     Scope: Global

 Candidate RP: 10.110.2.2 (Vlan-interface102)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:55
```

2. Verify that the RP has been elected in each zone to provide services for different multicast groups:

Display RP information on Switch B.

```
[SwitchB] display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 10.110.2.2
     Priority: 192
     HoldTime: 150
     Uptime: 00:03:39
     Expires: 00:01:51

 Group/MaskLen: 239.0.0.0/8
     RP: 10.110.1.2 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:07:44
     Expires: 00:01:51
```

Display RP information on Switch C.

```
[SwitchC] display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 10.110.2.2
     Priority: 192
     HoldTime: 150
     Uptime: 00:03:42
     Expires: 00:01:48

 Group/MaskLen: 239.0.0.0/8
     RP: 10.110.6.1 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:06:54
     Expires: 00:02:41
```

Display RP information on Switch E.

```
[SwitchE] display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 10.110.2.2 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:00:32
     Expires: 00:01:58
```

Display RP information on Switch F.

```
[SwitchF] display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
```

```
 Group/MaskLen: 224.0.0.0/4
     RP: 10.110.2.2
     Priority: 192
     HoldTime: 150
     Uptime: 00:04:30
     Expires: 00:02:23
```

The output shows the following:

- When a host in admin-scoped zone 1 joins a multicast group in the range of **239.0.0.0/8**, the RP (Switch B) provides services for this multicast group locally.
- When a host in admin-scoped zone 2 joins a multicast group in the range of **239.0.0.0/8**, the RP (Switch C) provides services for this multicast group locally.
- When a host in an admin-scoped zone or the global-scoped zone joins a multicast group out of the range of **239.0.0.0/8**, the RP (Switch E) provides services for this multicast group.

Configuration files

- Switch A:

```
#
multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 192.168.1.1 255.255.255.0
 igmp enable
 pim sm
#
interface Vlan-interface101
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
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
#
pim
 c-bsr admin-scope
#
```

- Switch B:

```
#
multicast routing-enable
#
acl number 2001
 rule 0 permit source 239.0.0.0 0.255.255.255
#
vlan 101 to 103
```

```
#
vlan 200
#
interface Vlan-interface101
 ip address 10.110.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 10.110.2.1 255.255.255.0
 multicast boundary 239.0.0.0 8
 pim sm
#
interface Vlan-interface103
 ip address 10.110.3.1 255.255.255.0
 multicast boundary 239.0.0.0 8
 pim sm
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.110.1.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
#
pim
 c-bsr admin-scope
 c-bsr group 239.0.0.0 255.0.0.0
 c-bsr vlan-interface 101
 c-rp vlan-interface 101 group-policy 2001
#
```

- Switch C:

```
#
multicast routing-enable
#
acl number 2001
 rule 0 permit source 239.0.0.0 0.255.255.255
#
vlan 104 to 106
#
vlan 300
#
interface Vlan-interface104
 ip address 10.110.4.1 255.255.255.0
 multicast boundary 239.0.0.0 8
```

```
 pim sm
#
interface Vlan-interface105
 ip address 10.110.5.1 255.255.255.0
 multicast boundary 239.0.0.0 8
 pim sm
#
interface Vlan-interface106
 ip address 10.110.6.1 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 10.110.4.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
  network 10.110.6.0 0.0.0.255
#
pim
 c-bsr admin-scope
 c-bsr group 239.0.0.0 255.0.0.0
 c-bsr vlan-interface 106
 c-rp vlan-interface 106 group-policy 2001
#
```

- Switch D:

```
#
multicast routing-enable
#
vlan 106
#
vlan 400
#
interface Vlan-interface106
 ip address 10.110.6.2 255.255.255.0
 pim sm
#
interface Vlan-interface400
 ip address 192.168.4.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.4.0 0.0.0.255
```

```
  network 10.110.6.0 0.0.0.255
#
pim
 c-bsr admin-scope
#
```

- Switch E:

```
#
multicast routing-enable
#
vlan 102
#
vlan 105
#
vlan 500
#
interface Vlan-interface102
 ip address 10.110.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 10.110.5.2 255.255.255.0
 pim sm
#
interface Vlan-interface500
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.5.0 0.0.0.255
  network 10.110.2.0 0.0.0.255
  network 10.110.5.0 0.0.0.255
#
pim
 c-bsr admin-scope
 c-bsr global
 c-bsr vlan-interface 102
 c-rp vlan-interface 102
#
```

- Switch F:

```
#
multicast routing-enable
#
vlan 103 to 104
#
vlan 600
#
interface Vlan-interface103
```

```
 ip address 10.110.3.2 255.255.255.0
 pim sm
#
interface Vlan-interface104
 ip address 10.110.4.2 255.255.255.0
 pim sm
#
interface Vlan-interface600
 ip address 192.168.6.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
  network 192.168.6.0 0.0.0.255
  network 10.110.3.0 0.0.0.255
  network 10.110.4.0 0.0.0.255
#
pim
 c-bsr admin-scope
#
```

Example: Configuring PIM-SSM

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 169:

- All switches are Layer 3 switches, and they run OSPF.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.
- The receiver hosts in the user networks support IGMPv3.

Configure PIM-SSM on each switch, so that the receiver hosts can receive VOD streams destined for a multicast group in the SSM group range **232.1.1.0/24** from a specific multicast source.

Figure 169 Network diagram

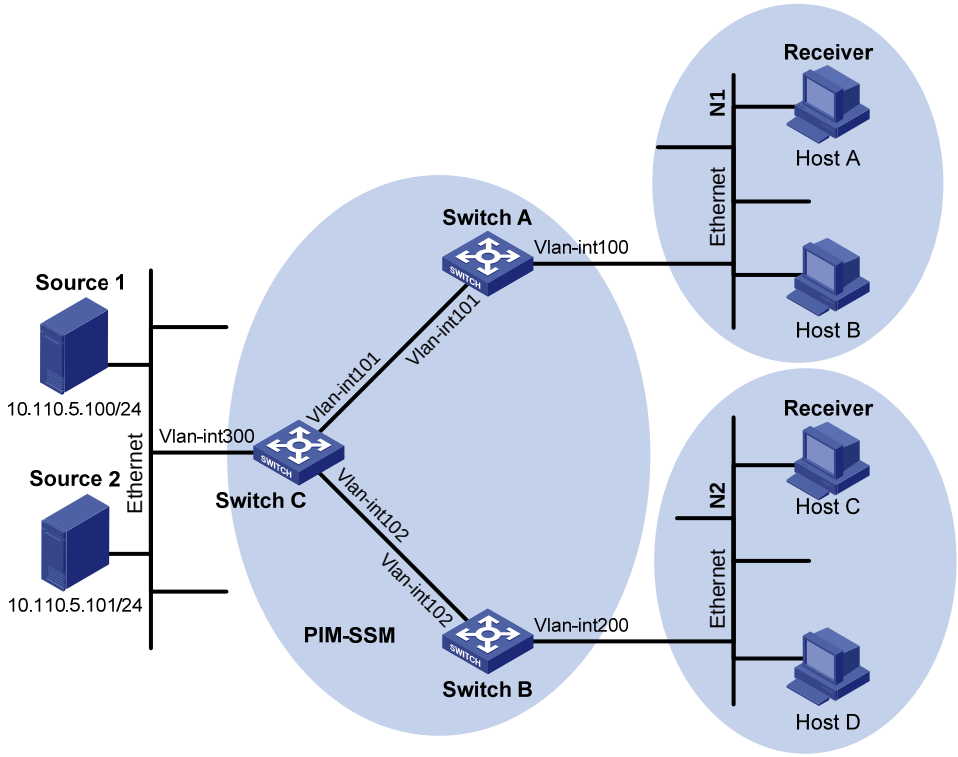


Table 20 IP address assignment

Device	Interface	IP address
Switch A	VLAN-interface 100	10.110.1.1/24
Switch A	VLAN-interface 101	192.168.1.1/24
Switch B	VLAN-interface 200	10.110.2.1/24
Switch B	VLAN-interface 102	192.168.2.1/24
Switch C	VLAN-interface 300	10.110.5.1/24
Switch C	VLAN-interface 101	192.168.1.2/24
Switch C	VLAN-interface 102	192.168.2.2/24

Requirements analysis

For PIM-SSM to provide services for multicast groups in the range specified in the network requirements, you must specify this range on each Layer 3 switch.

In SSM, the edge Layer 3 switch must get information about the specified multicast source when a host joins a multicast group. To meet the requirement, you must enable IGMPv3 on the edge switches that connect to the user networks.

Configuration restrictions and guidelines

When a member of a multicast group in the SSM group range sends an IGMPv1 or IGMPv2 report message, the switch does not trigger a (*, G) join message. In this case, you can configure IGMP SSM mappings, so that PIM-SSM can provide services for hosts that support IGMPv1 or IGMPv2.

Configuration procedures

1. Assign an IP address and subnet mask to each interface according to Table 20. (Details not shown.)
2. Configure OSPF on the switches in the PIM-SSM domain. (Details not shown.)
3. Enable IP multicast routing and PIM-SSM on each switch:

   # On Switch A, enable IP multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing-enable
   ```

   # On Switch A, enable PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] pim sm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim sm
   [SwitchA-Vlan-interface101] quit
   ```

   # On Switch B and Switch C, enable IP multicast routing and PIM-SM in the same way Switch A is configured. (Details not shown.)
4. Configure the SSM group range:

   # On Switch A, configure the SSM group range to be **232.1.1.0/24**.

   ```
   [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
   [SwitchA-pim] quit
   ```

   # On Switch B and Switch C, configure the SSM group range in the same way Switch A is configured. (Details not shown.)
5. Enable IGMPv3 on the interfaces that are directly connected to user networks:

   # On Switch A, enable IGMPv3 on VLAN-interface 100. (By default, the IGMP version is 2.)

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] igmp enable
   [SwitchA-Vlan-interface100] igmp version 3
   [SwitchA-Vlan-interface100] quit
   ```

   # On Switch B, enable IGMPv3 on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

To verify that correct (S, G) entries can be created on switches:

1. Send IGMPv3 report from Host A to join the multicast group **232.1.1.1** and specify the multicast source as **10.110.5.100/24**.
2. Use the **display pim routing-table** command to display PIM routing tables on Switch A and Switch C:

   # Display the PIM routing table on Switch A.

```
[SwitchA] 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: 00:13:25
     Upstream interface: Vlan-interface101
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface100
                  Protocol: igmp, UpTime: 00:13:25, Expires: -
```

   # Display the PIM routing table on Switch C.

```
[SwitchC] display pim routing-table
 VPN-Instance: public net
 Total entry; 1 (S, G) entry

 (10.110.5.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:LOC
     UpTime: 00:12:05
     Upstream interface: Vlan-interface300
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan-interface101
                  Protocol: pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

   The output shows that Switch A builds an SPT toward the multicast source. Switches on the SPT path (Switch A and Switch D) generate (S, G) entries.

Configuration files

- Switch A:

```
#
multicast routing-enable
#
acl number 2000
```

```
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp version 3
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
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
#
pim
 ssm-policy 2000
#
```

- Switch B:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp version 3
 pim sm
#
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
 ssm-policy 2000
#
```

- Switch C:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.5.0 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
#
```

Port isolation configuration examples

This chapter provides port isolation configuration examples.

The port isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs. You can also use this feature to isolate the hosts in a VLAN from one another.

Example: Configuring port isolation

Applicable product matrix

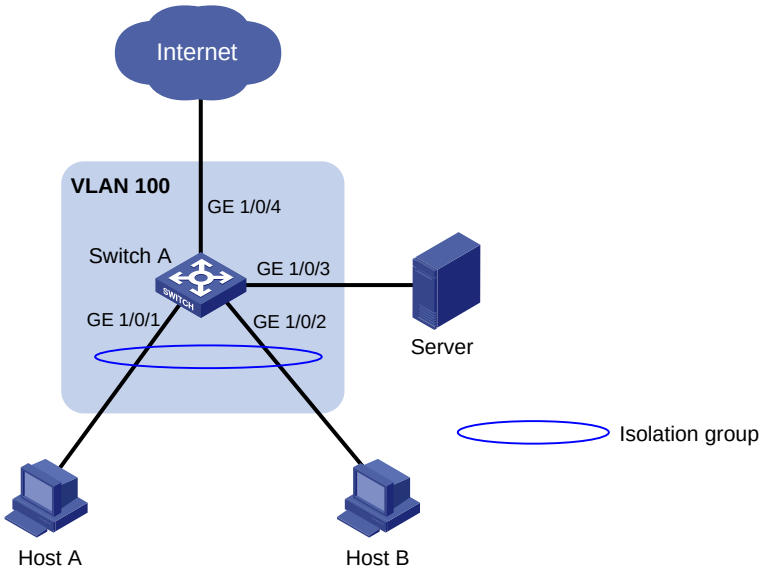
Product series	Software version
HP 7500	Release series 6620
	Release series 6630
	Release series 6700

Network requirements

As shown in Figure 170, Host A and host B are in the same VLAN.

Configure port isolation on Switch A to provide access to the Internet and the server for both hosts, and isolate them from each other.

Figure 170 Network diagram



Configuration restrictions and guidelines

When you configure port isolation, follow these restrictions and guidelines:

- Before you assign a port to the isolation group, make sure the port is operating in **bridge** mode.

- You cannot assign the member ports of a service loopback group to the isolation group, and vice versa.

Configuration procedures

Create VLAN 100, and then assign ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the VLAN.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] quit
```

Assign ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the isolation group.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port-isolate enable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port-isolate enable
[SwitchA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about the isolation group.

```
<SwitchA> display port-isolate group
 Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1     GigabitEthernet1/0/2
```

Configuration files

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
```

```
 port link-mode bridge
 port access vlan 100
#
```

Example: Implementing time-based access control for isolated ports

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

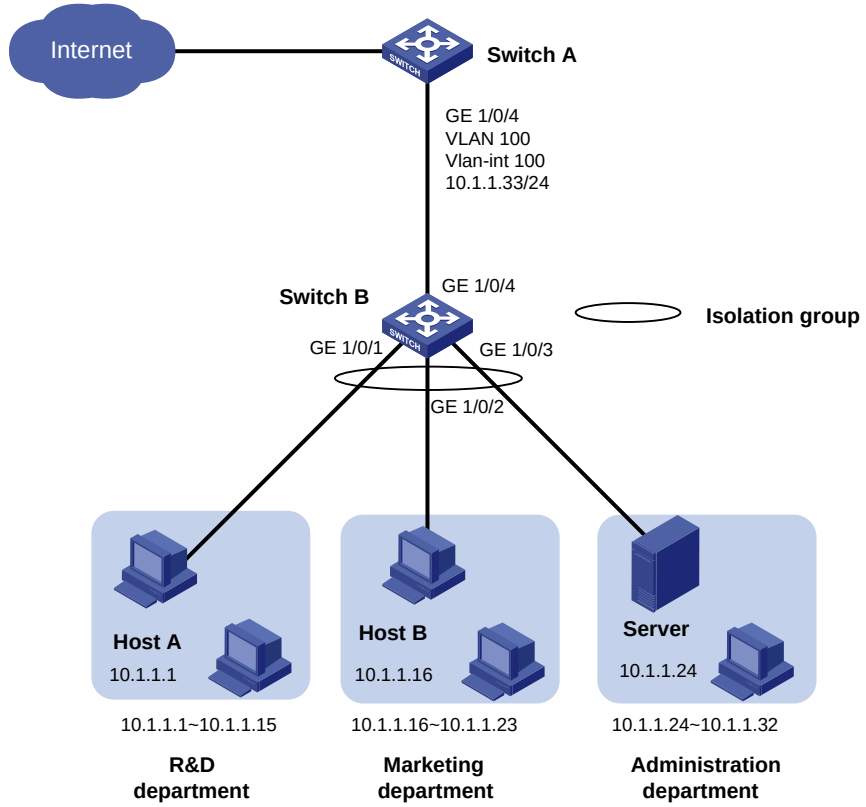
As shown in Figure 171:

- The R&D department, Marketing department, and Administration department are connected to Switch B.
- Host A, Host B, and the server are located in the R&D department, Marketing department, and Administration department, respectively.

Configure port isolation on Switch B and other features on Switch A to meet the following requirements:

- Hosts in all three departments can access the Internet.
- Every day from 8:00 to 12:00, only host A can access the server in the administration department.
- Every day from 14:00 to 16:00, only host B can access the server in the administration department.
- All cross-department communications at any other times are denied.

Figure 171 Network diagram



Requirement analysis

To enable ports in the isolation group to access each other at Layer 3, enable local proxy ARP on the gateway device.

To enable the isolated ports to access each other only at specified time ranges, configure a time-based ACL on the gateway device.

Configuration procedures

1. Configure Switch B:

   # Add ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to VLAN 100.

   ```
   <SwitchB> system-view
   [SwitchB] vlan 100
   [SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
   [SwitchB-vlan100] quit
   ```

   # Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the isolation group to disable host A and host B from accessing the server at Layer 2.

   ```
   [SwitchB] interface gigabitethernet 1/0/1
   [SwitchB-GigabitEthernet1/0/1] port-isolate enable
   [SwitchB-GigabitEthernet1/0/1] quit
   [SwitchB] interface gigabitethernet 1/0/2
   [SwitchB-GigabitEthernet1/0/2] port-isolate enable
   [SwitchB-GigabitEthernet1/0/2] quit
   ```

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port-isolate enable
[SwitchB-GigabitEthernet1/0/3] quit
```

2. Configure Switch A:

Configure the IP address and mask of VLAN interface 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/4
[SwitchA-vlan100] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.33 255.255.255.0
```

Enable local proxy ARP on VLAN interface 100 to enable host A and host B to access the server at Layer 3.

```
[SwitchA-Vlan-interface100] local-proxy-arp enable
[SwitchA-Vlan-interface100] quit
```

Create two periodic time ranges: **trname_1**, which is active from 8:00 to 12:00 every day, and **trname_2**, which is active from 14:00 to 16:00 every day.

```
[SwitchA] time-range trname_1 8:00 to 12:00 daily
[SwitchA] time-range trname_2 14:00 to 16:00 daily
```

Create IPv4 ACL 3000.

```
[SwitchA] acl number 3000
```

Configure one rule to permit access from host A to the server from 8:00 to 12:00 every day.

```
[SwitchA-acl-adv-3000] rule permit ip source 10.1.1.1 0 destination 10.1.1.24 0
time-range trname_1
```

Configure one rule to permit access from host B to the server from 14:00 to 16:00 every day.

```
[SwitchA-acl-adv-3000] rule permit ip source 10.1.1.16 0 destination 10.1.1.24 0
time-range trname_2
```

Configure one rule to deny all cross-department communications.

```
[SwitchA-acl-adv-3000] rule deny ip source 10.1.1.0 0.0.0.31 destination 10.1.1.0
0.0.0.31
[SwitchA-acl-adv-3000] quit
```

Apply the IPv4 advanced ACL 3000 to GigabitEthernet 1/0/4 to filter incoming packets.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] packet-filter 3000 inbound
```

Verifying the configuration

1. On Switch B:

Display information about the isolation group.

```
[SwitchB]display port-isolate group
 Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1    GigabitEthernet1/0/2    GigabitEthernet1/0/3
```

2. On Switch A:

Display information about VLAN 100.

```
   [SwitchA-Vlan-interface100]display this
```

```
#
interface Vlan-interface100
 ip address 10.1.1.33 255.255.255.0
 local-proxy-arp enable
#
return
```

Display ACL rules of ACL 3000.

```
[SwitchA]display acl 3000
Advanced ACL  3000, named -none-, 3 rules,
ACL's step is 5
 rule 0 permit ip source 10.1.1.1 0 destination 10.1.1.24 0 time-range trname_1
 rule 5 permit ip source 10.1.1.16 0 destination 10.1.1.24 0 time-range trname_2
 rule 10 deny ip source 10.1.1.0 0.0.0.31 destination 10.1.1.0 0.0.0.31
```

Configuration files

- Switch B:

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
```

- Switch A:

```
#
 time-range trname_1_8:00 to 12:00 daily
 time-range trname_2 14:00 to 16:00 daily
#
acl number 3000
 rule 0 permit ip source 10.1.1.1 0 destination 10.1.1.24 0 time-range trname_1
 rule 5 permit ip source 10.1.1.16 0 destination 10.1.1.24 0 time-range trname_2
 rule 10 deny ip source 10.1.1.0 0.0.0.31 destination 10.1.1.0 0.0.0.31
```

```
#
vlan 100
#
interface Vlan-interface 100
 ip address 10.1.1.33 255.255.255.0
 local-proxy-arp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
 packet-filter 3000 inbound
#
```

Port security configuration examples

This chapter provides examples for configuring port security modes to control network access of users.

General configuration restrictions and guidelines

When you configure port security, follow these restrictions and guidelines:

- Disable global 802.1X and MAC authentications before you enable port security on a port.
- When port security is enabled, you cannot do any of the following:
  - Manually enable 802.1X or MAC authentication.
  - Change the access control mode.
  - Change the port authorization state.

  The port security feature modifies these settings automatically in different security modes.
- You cannot disable port security when online users are present.
- Port security modes are mutually exclusive with link aggregation and service loopback groups.
- The maximum number of users a port supports equals one of the following (whichever is smaller):
  - The maximum number of secure MAC addresses that the port security allows.
  - The maximum number of concurrent users the authentication mode in use allows.

  For example, the port security's limit takes effect if 802.1X allows more concurrent users than the port security's limit on the number of MAC addresses on the port in userLoginSecureExt mode.

Example: Configuring autoLearn mode

Applicable product matrix

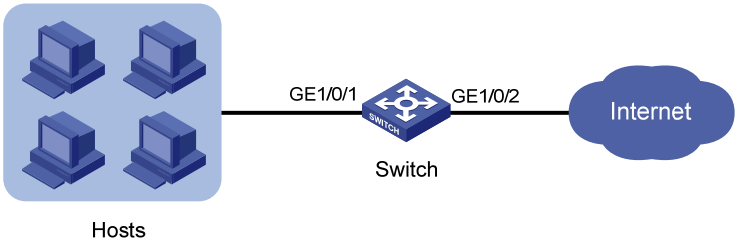
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 172, configure port security mode **autoLearn** on the switch to meet the following requirements:

- The switch accepts a maximum of 64 users to log in without authentication.
- After the number of users reaches 64, the port denies any new users access to the Internet.

Figure 172 Network diagram



Requirements analysis

Because the hosts are connected to GigabitEthernet 1/0/1, configure the autoLearn mode on that port.

To meet the requirements for configuring autoLearn mode, do the following:

- To update MAC address table, configure an aging timer for the secure MAC addresses. This example uses 30 minutes.
- To deny any new users access to the Internet after the number of online users reaches 64, do the following:
  - Enable intrusion traps.
  - Configure the port to shut down temporarily for 30 seconds.

Configuration restrictions and guidelines

When you configure the autoLearn mode, follow these restrictions and guidelines:

- To change the security mode of a port security-enabled port, first set the port in noRestrictions mode. You can use the **undo port-security port-mode** command to set the port in noRestrictions mode.
- Before you enable the autoLearn mode, set the port security's limit on the number of MAC addresses by using the **port-security max-mac-count** command. You cannot change the setting when the port is operating in autoLearn mode.

Configuration procedures

Enter system view.

```
<Switch> system-view
[Switch]
```

Set the secure MAC aging timer to 30 minutes.

```
[Switch] port-security timer autolearn aging 30
```

Set the port security's limit on the number of secure MAC addresses to 64 on port GigabitEthernet 1/0/1.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to **autoLearn**.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-GigabitEthernet1/0/1] quit
```

```
[Switch] port-security timer disableport 30
```

Enable intrusion traps and port security. The port security module sends traps when it detects illegal frames.

```
[Switch] port-security trap intrusion
[Switch] port-security enable
 Please wait.............................. Done.
```

Verifying the configuration

Display the port security configuration.

```
<Switch> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Intrusion trap is enabled
 AutoLearn aging time is 30 minutes
 Disableport Timeout: 30s
 OUI value:

GigabitEthernet1/0/1 is link-up
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is DisablePortTemporarily
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

The output shows the following:

- The port security's limit on the number of secure MAC addresses on the port is 64.
- The port security mode is autoLearn.
- The intrusion protection action is disabling the port (DisablePortTemporarily) for 30 seconds.

The port allows for MAC address learning, and you can view the number of learned MAC addresses in the message "Stored MAC address number is *n*".

Use the **display port-security** command repeatedly to track the number of MAC addresses learned by the port.

Use the **display this** command in interface view to display the learned secure MAC addresses.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security intrusion-mode disableport-temporarily
 port-security mac-address security sticky 0002-0000-0015 vlan 1
 port-security mac-address security sticky 0002-0000-0014 vlan 1
```

```
 port-security mac-address security sticky 0002-0000-0013 vlan 1
 port-security mac-address security sticky 0002-0000-0012 vlan 1
 port-security mac-address security sticky 0002-0000-0011 vlan 1
#
```

Use the **display port-security interface** command after the number of MAC addresses learned by the port reaches 64. You can see that the port security mode is changed to **secure**. When a frame with an unknown MAC address arrives, intrusion protection is triggered. The following trap is sent:

```
#Apr 26 12:47:14:210 2000 Switch PORTSEC/4/VIOLATION:
Trap1.3.6.1.4.1.25506.2.26.1.3.2
 An intrusion occurs!
 IfIndex: 17825797
 Port: 17825797
 MAC Addr: E8:39:35:5F:31:91
 VLAN ID: 1
 IfAdminStatus: 2
```

Use the **display interface** command. The output shows that the port is disabled.

```
<Switch> display interface gigabitethernet 1/0/1
 gigabitEthernet1/0/1 current state: DOWN (  Port Security Disabled  )
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8927-ad7d
 Description: GigabitEthernet1/0/1 Interface ......
```

Use the **display interface** command after 30 seconds. The output shows that the interface is enabled.

```
[Switch-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface
 ......
```

Use the **undo port-security mac-address security** command to delete several secure MAC addresses. The port security mode of the port changes to **autoLearn**, and the port can learn MAC addresses again.

Configuration files

```
#
 port-security enable
 port-security trap intrusion
 port-security timer autolearn aging 30
 port-security timer disableport 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security intrusion-mode disableport-temporarily
#
```

Example: Configuring userLoginWithOUI mode

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

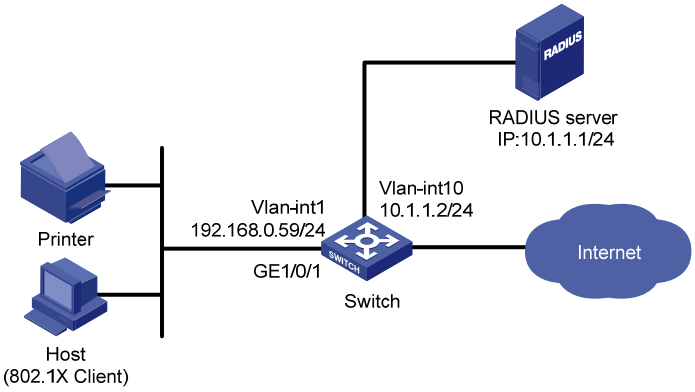
Network requirements

As shown in Figure 173, the switch uses the RADIUS server to authenticate users. The users use 802.1X client to initiate authentication.

Configure port security mode **userLoginWithOUI** on the switch to meet the following requirements:

- Permit only one 802.1X user to pass authentication to access the Internet.
- Permit the printer to access the Internet.
- Perform the **blockmac** intrusion protection. The switch does the following:
  - Adds the source MAC addresses of illegal frames to the blocked MAC addresses list.
  - Discards all frames sourced from the blocked MAC addresses.

Figure 173 Network diagram



Requirements analysis

Because the hosts are connected to GigabitEthernet 1/0/1, configure the userLoginWithOUI mode on that port.

To meet the requirements for configuring userLoginWithOUI mode, do the following:

- To permit the printer to access the Internet, add the OUI of the printer to the switch. To match the OUIs of different printer vendors, add multiple OUIs to the switch.
- To perform RADIUS-based authentication, configure a RADIUS scheme and specify an authentication domain.

Configuration restrictions and guidelines

When you configure the userLoginWithOUI mode, follow these restrictions and guidelines:

- To change the security mode of a port security-enabled port, first set the port in noRestrictions mode . You can use the **undo port-security port-mode** command to set the port in noRestrictions mode.
- The authentication port (UDP) used by RADIUS servers is 1812, according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. Configure the port used for RADIUS authentication to 1645 for the RADIUS scheme on the switch.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring IP addresses

Assign an IP address to each interface, as shown in Figure 173. Make sure the host, printer, switch, and RADIUS server can reach each other. (Details not shown.)

Configuring the switch

1. Configure the RADIUS scheme:

   # Create RADIUS scheme **radsun**.

   ```
   <Switch> system-view
   [Switch] radius scheme radsun
   New Radius scheme
   ```

   # Specify the RADIUS server at 10.1.1.1 as the primary authentication server, and set the shared authentication key to **aabbcc**.

   ```
   [Switch-radius-radsun] primary authentication 10.1.1.1 1645 key aabbcc
   ```

   # Set the response timeout time of the RADIUS server to 5 seconds.

   ```
   [Switch-radius-radsun] timer response-timeout 5
   ```

   # Set the maximum number of RADIUS packet retransmission attempts to 5.

   ```
   [Switch-radius-radsun] retry 5
   ```

   # Configure the switch to send usernames without domain names to the RADIUS server.

   ```
   [Switch-radius-radsun] user-name-format without-domain
   [Switch-radius-radsun] quit
   ```

   # Create ISP domain **sun** and enter ISP domain view.

   ```
   [Switch] domain sun
   [Switch-isp-sun]
   ```

   # Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication and authorization of all LAN-access users.

   ```
   [Switch-isp-sun] authentication default radius-scheme radsun
   [Switch-isp-sun] authorization default radius-scheme radsun
   [Switch-isp-sun] accounting default none
   [Switch-isp-sun] quit
   ```

2. Set the 802.1X authentication method to CHAP. This configuration is optional because by default, the authentication method is CHAP for 802.1X.

   ```
   [Switch] dot1x authentication-method chap
   ```

```
CHAP authentication enabled already.
```

3. Configure port security:

   # Add five OUI values.

```
[Switch] port-security oui 1234-0100-1111 index 1
[Switch] port-security oui 1234-0200-1111 index 2
[Switch] port-security oui 1234-0300-1111 index 3
[Switch] port-security oui 1234-0400-1111 index 4
[Switch] port-security oui 1234-0500-1111 index 5
```

   # Set the port security mode to **userLoginWithOUI**.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

   # Configure port GigabitEthernet 1/0/1 to perform the **blockmac** intrusion protection feature.

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
[Switch-GigabitEthernet1/0/1] quit
```

   # Enable port security.

```
[Switch] port-security enable
 Please wait.............................. Done.
```

Configuring the RADIUS server

Create RADIUS user **aaa** on the RADIUS server, and enter RADIUS-server user view.

```
<Sysname> system-view
[Sysname] radius-server user aaa
[Sysname-rdsuser-aaa]
```

Set the password to **123456** in plain text for RADIUS user **aaa**.

```
[Sysname-rdsuser-aaa] password simple 123456
[Sysname-rdsuser-aaa] quit
```

Specify RADIUS client **10.1.1.2**, and set the shared key to **aabbcc** in plain text.

```
[Sysname] radius-server client-ip 10.1.1.2 key simple aabbcc
```

Verifying the configuration

Display the RADIUS scheme **radsun**.

```
[Switch] display radius scheme radsun
SchemeName   : radsun
  Index : 1                           Type : standard
  Primary Auth Server:
    IP: 10.1.1.1                                  Port: 1645   State: active
    Encryption Key : ******
    VPN instance   : N/A
    Probe username : N/A
    Probe interval : N/A
  Auth Server Encryption Key : N/A
  Acct Server Encryption Key : N/A
  VPN instance               : N/A
  Accounting-On packet disable, send times : 50 , interval : 3s
  Interval for timeout(second)                          : 5
  Retransmission times for timeout                      : 5
```

```
  Interval for realtime accounting(minute)               : 12
  Retransmission times of realtime-accounting packet     : 5
  Retransmission times of stop-accounting packet         : 500
  Quiet-interval(min)                                    : 5
  Username format                                        : without-domain
  Data flow unit                                         : Byte
  Packet unit                                            : one
```

Display the configuration of the ISP domain **sun**.

```
<Switch> display domain sun
   Domain: sun
   State: Active
   Access-limit: Disabled
   Accounting method: Required
   Default authentication scheme      : radius:radsun
   Default authorization scheme       : radius:radsun
   Default accounting scheme          : none
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes:
```

Display the port security configuration.

```
<Switch> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 123401
   Index is 2,  OUI value is 123402
   Index is 3,  OUI value is 123403
   Index is 4,  OUI value is 123404
   Index is 5,  OUI value is 123405

 GigabitEthernet1/0/1 is link-up
   Port mode is userLoginWithOUI
   NeedToKnow mode is disabled
   Intrusion Protection mode is BlockMacAddress
   Max MAC address number is not configured
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

After an 802.1X user goes online, you can see that the number of secure MAC addresses saved by the port is 1.

Display 802.1X information.

```
<Switch> display dot1x interface gigabitethernet 1/0/1
 Equipment 802.1X protocol is enabled
```

```
 CHAP authentication is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD quick deploy is disabled

Configuration: Transmit Period   30 s,  Handshake Period       15 s
               Quiet Period      60 s,  Quiet Period Timer is disabled
               Supp Timeout      30 s,  Server Timeout        100 s
               Reauth Period   3600 s
               The maximal retransmitting times    2
EAD quick deploy configuration:
               EAD timeout:   30 m

 Total maximum 802.1X user resource number is 2048 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Proxy trap checker is   disabled
   Proxy logoff checker is disabled
   Handshake is enabled
   Handshake secure is disabled
   802.1X unicast-trigger is enabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   802.1X Multicast-trigger is enabled
   Mandatory authentication domain: NOT configured
   Guest VLAN: NOT configured
   Auth-Fail VLAN: NOT configured
   Critical VLAN: NOT configured
   Critical recovery-action: NOT configured
   Max number of on-line users is 1024

   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
        EAP Success Packets: 4, Fail Packets: 5
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

   Controlled User(s) amount to 1
```

The port also allows an additional user whose MAC address has an OUI among the specified OUIs to pass authentication.

Display the MAC address information for interface GigabitEthernet 1/0/1.

```
<Switch> display mac-address interface gigabitethernet 1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
1234-0300-0011  1         Learned        GigabitEthernet1/0/1     AGING

  ---  1 mac address(es) found  ---
```

Configuration files

```
#
 port-security enable
 port-security oui 1234-0100-0000 index 1
 port-security oui 1234-0200-0000 index 2
 port-security oui 1234-0300-0000 index 3
 port-security oui 1234-0400-0000 index 4
 port-security oui 1234-0500-0000 index 5
#
radius scheme radsun
 primary authentication 10.1.1.1 1645 key cipher $c$3$krBjik3mdDkyVGW9JRInyID3GMYJOw==
 timer response-timeout 5
 user-name-format without-domain
 retry 5
#
domain sun
 authentication default radius-scheme radsun
 authorization default radius-scheme radsun
 accounting default none
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security port-mode userlogin-withoui
 port-security intrusion-mode blockmac
#
```

Example: Configuring macAddressOrUserLoginSecure mode

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

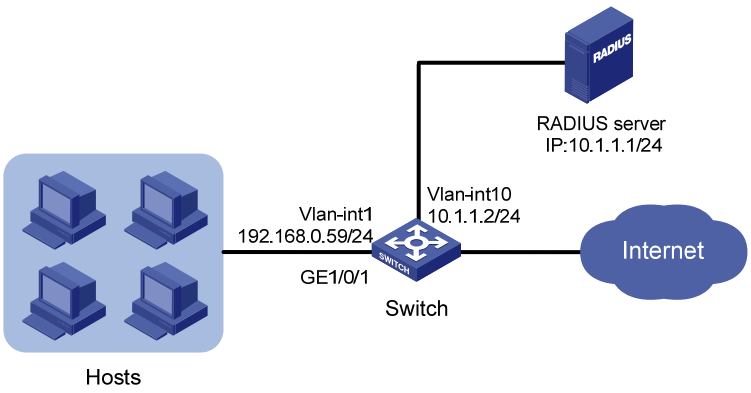
Network requirements

As shown in Figure 174, the switch uses the RADIUS server to authenticate users.

Configure port security mode **macAddressOrUserLoginSecure** on the switch to meet the following requirements:

- Allow only one 802.1X user to pass authentication, and allows multiple MAC authentication users to pass authentication.
- Use shared user account with username **aaa** and password **123456** for MAC authentication users.
- Allow a maximum of 64 authenticated users.
- Perform the **ntkonly** feature to prevent frames from being sent to unknown MAC addresses.

Figure 174 Network diagram



Requirements analysis

Because the hosts are connected to GigabitEthernet 1/0/1 of the switch, configure the macAddressOrUserLoginSecure mode on that port.

To perform RADIUS-based authentication, configure a RADIUS scheme and specify an authentication domain.

Configuration restrictions and guidelines

When you configure the macAddressOrUserLoginSecure mode, follow these restrictions and guidelines:

- To change the security mode of a port security-enabled port, first set the port in noRestrictions mode. You can use the **undo port-security port-mode** command to set the port in noRestrictions mode.
- The authentication port (UDP) used by RADIUS servers is 1812, according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. Configure the port used for RADIUS authentication to 1645 for the RADIUS scheme on the switch.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring IP addresses

Assign an IP address to each interface, as shown in Figure 174. Make sure the hosts, switch, and RADIUS server can reach each other. (Details not shown.)

Configuring the switch

1. Configure the RADIUS scheme:

   # Create RADIUS scheme **radsun**.

   ```
   <Switch> system-view
   [Switch] radius scheme radsun
   New Radius scheme
   ```

   # Specify the RADIUS server at 10.1.1.1 as the primary authentication server, and set the shared authentication key to **aabbcc**.

   ```
   [Switch-radius-radsun] primary authentication 10.1.1.1 1645 key aabbcc
   ```

   # Set the response timeout time of the RADIUS server to 5 seconds.

   ```
   [Switch-radius-radsun] timer response-timeout 5
   ```

   # Set the maximum number of RADIUS packet retransmission attempts to five.

   ```
   [Switch-radius-radsun] retry 5
   ```

   # Configure the switch to send usernames without domain names to the RADIUS server.

   ```
   [Switch-radius-radsun] user-name-format without-domain
   [Switch-radius-radsun] quit
   ```

   # Create ISP domain **sun** and enter ISP domain view.

   ```
   [Switch] domain sun
   [Switch-isp-sun]
   ```

   # Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication and authorization of all LAN-access users.

   ```
   [Switch-isp-sun] authentication lan-access radius-scheme radsun
   [Switch-isp-sun] authorization lan-access radius-scheme radsun
   [Switch-isp-sun] accounting lan-access none
   [Switch-isp-sun] quit
   ```

2. Configure port security:

   # Set the 802.1X authentication method to CHAP. This step is optional because by default, the authentication method is CHAP for 802.1X.

   ```
   [Switch] dot1x authentication-method chap
   CHAP authentication enabled already.
   ```

   # Specify ISP domain **sun** for MAC authentication.

```
[Switch] mac-authentication domain sun
```

Configure the username and password for MAC authentication as **aaa** and **123456**.

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
```

Set the port security's limit on the number of secure MAC addresses to 64 on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to **macAddressOrUserLoginSecure**.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-secure-or-mac
```

Set the NTK mode of the port to **ntkonly**.

```
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Switch-GigabitEthernet1/0/1] quit
```

Enable port security.

```
[Switch] port-security enable
 Please wait.............................. Done.
```

Configuring the RADIUS server

Create RADIUS user **aaa** on the RADIUS server, and enter RADIUS-server user view.

```
<Sysname> system-view
[Sysname] radius-server user aaa
[Sysname-rdsuser-aaa]
```

Set the password to **123456** in plain text for RADIUS user **aaa**.

```
[Sysname-rdsuser-aaa] password simple 123456
[Sysname-rdsuser-aaa] quit
```

Specify RADIUS client **10.1.1.2**, and set the shared key to **aabbcc** in plain text.

```
[Sysname] radius-server client-ip 10.1.1.2 key simple aabbcc
```

Verifying the configuration

Display the port security configuration.

```
<Switch> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:

 GigabitEthernet1/0/1 is link-up
   Port mode is macAddressOrUserLoginSecure
   NeedToKnow mode is NeedToKnowOnly
   Intrusion Protection mode is NoAction
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

Display MAC authentication information.

```
<Switch> display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
 User name format is fixed account
 Fixed username:aaa
 Fixed password: ******
          Offline detect period is 300s
          Quiet period is 60s
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 3
          Current domain is sun

Silent MAC User info:
          MAC Addr         From Port                    Port Index

GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 3, failed: 1
  Max number of on-line users is 1024
Current online user number is 32
          MAC Addr         Authenticate State           Auth Index
          1234-0300-0011   MAC_AUTHENTICATOR_SUCCESS     13
          1234-0300-0012   MAC_AUTHENTICATOR_SUCCESS     14
          1234-0300-0013   MAC_AUTHENTICATOR_SUCCESS     15
```

Display 802.1X authentication information.

```
<Switch> display dot1x interface gigabitethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD quick deploy is disabled

 Configuration: Transmit Period   30 s,  Handshake Period       15 s
                Quiet Period      60 s,  Quiet Period Timer is disabled
                Supp Timeout      30 s,  Server Timeout        100 s
                Reauth Period   3600 s
                The maximal retransmitting times    2
 EAD quick deploy configuration:
                EAD timeout:   30 m

 The maximum 802.1X user resource number is 2048 per slot
 Total current used 802.1X resource number is 1

GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Proxy trap checker is   disabled
   Proxy logoff checker is disabled
   Handshake is enabled
```

```
  Handshake secure is disabled
  802.1X unicast-trigger is enabled
  Periodic reauthentication is disabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  802.1X Multicast-trigger is enabled
  Mandatory authentication domain: NOT configured
  Guest VLAN: NOT configured
  Auth-Fail VLAN: NOT configured
  Critical VLAN: NOT configured
  Critical recovery-action: NOT configured
  Max number of on-line users is 1024

  EAPOL Packet: Tx 16331, Rx 102
  Sent EAP Request/Identity Packets : 16316
       EAP Request/Challenge Packets: 6
       EAP Success Packets: 4, Fail Packets: 5
  Received EAPOL Start Packets : 6
           EAPOL LogOff Packets: 2
           EAP Response/Identity Packets : 80
           EAP Response/Challenge Packets: 6
           Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

  Controlled User(s) amount to 1
```

Because NTK is enabled, frames with an unknown destination MAC address, multicast address, or broadcast address are discarded.

Configuration files

```
#
 port-security enable
#
 mac-authentication domain sun
 mac-authentication user-name-format fixed account aaa password cipher
$c$3$6DXUG/ZZMl7AbkMpJEo2uoni19WCI0nJGw
#
radius scheme radsun
 primary authentication 10.1.1.1 1645 key cipher $c$3$krBjik3mdDkyVGW9JRInyID3GMYJOw==
 timer response-timeout 5
 user-name-format without-domain
 retry 5
#
domain sun
 authentication lan-access radius-scheme radsun
 authorization lan-access radius-scheme radsun
 accounting lan-access none
 access-limit disable
```

```
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security max-mac-count 64
 port-security port-mode userlogin-secure-or-mac
 port-security ntk-mode ntkonly
#
```

QinQ configuration examples

This chapter provides examples for using QinQ to extend customer VLANs (CVLANs) across an Ethernet service provider network.

QinQ enables service providers to separate or aggregate customer traffic in the service provider network by adding a layer of service provider VLAN tag (SVLAN tag) to customer traffic.

QinQ has the following implementations:

- **Basic QinQ**—Enabled on a per-port basis. A basic QinQ-enabled port tags all incoming frames (tagged or untagged) with the PVID tag without discriminating between CVLANs. As a result, basic QinQ cannot separate a customer's traffic by traffic type.
- **Selective QinQ**—Implemented through QoS policies. Selective QinQ enables a port to tag incoming traffic with different SVLAN tags for different CVLANs. In contrast to basic QinQ, selective QinQ can separate traffic by both customer and traffic type.

Use basic QinQ to separate traffic by customer.

Use selective QinQ to separate traffic by CVLAN for a customer that has multiple CVLANs.

NOTE:

On a QinQ-enabled port, the device learns MAC addresses to SVLANs instead of CVLANs.

Example: Configuring basic QinQ

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

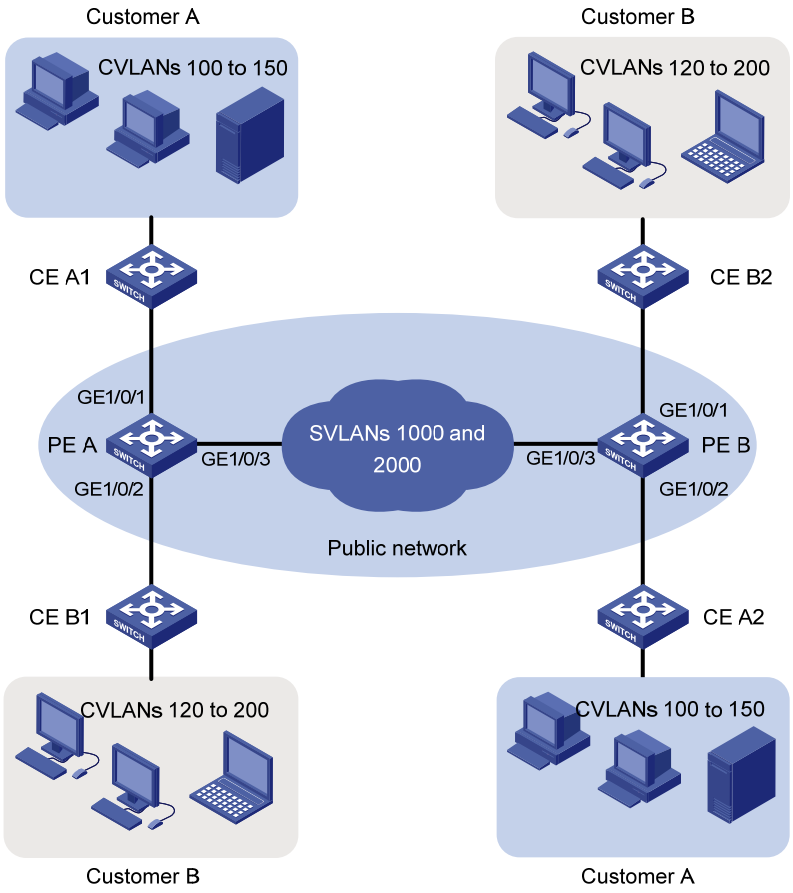
Network requirements

As shown in Figure 175, Customer A and Customer B each have two branches.

Configure basic QinQ on PE A and PE B to provide Layer 2 connectivity for Customer A and Customer B over the service provider network.

In the service provider network, assign VLAN 1000 and VLAN 2000 to Customer A and Customer B, respectively.

Figure 175 Network diagram



Requirements analysis

To run QinQ, you only need to configure QinQ on customer-side ports of PEs.

For the customer-side hybrid ports to send traffic to the customer site with the SVLAN tag removed, you must assign the ports to the SVLANs (port VLANs) as untagged VLAN members.

For the service provider-side ports to support multiple SVLANs, configure the link type of service provider-side ports as trunk or hybrid.

To send QinQ frames across the service provider network, you must configure all the ports on the forwarding path to allow frames from VLAN 1000 and VLAN 2000 to pass through without removing the VLAN tag.

Configuration restrictions and guidelines

When you configure basic QinQ, follow these restrictions and guidelines:

- The link type of customer-side ports can be access, hybrid, or trunk. Whichever link type you choose, basic QinQ tags incoming frames (tagged or untagged) with the PVID tag.
- On a basic QinQ-enabled port, you must set the SVLAN ID as the PVID.
- You must set the MTU to at least 1504 bytes for each port on the path of QinQ frames in the service provider network.

Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

Configuring PE A

1. Create VLAN 1000 and VLAN 2000.

```
<PE_A> system-view
[PE_A] vlan 1000
[PE_A-vlan1000] quit
[PE_A] vlan 2000
[PE_A-vlan2000] quit
```

2. Configure GigabitEthernet 1/0/1 (a customer-side port):

   # Configure the port as a hybrid port, and set its PVID to 1000.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-GigabitEthernet1/0/1] port hybrid pvid vlan 1000
```

   # Remove the port from VLAN 1, and assign it to VLAN 1000 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

   # Enable basic QinQ on the port.

```
[PE_A-GigabitEthernet1/0/1] qinq enable
[PE_A-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

   # Configure the port as an access port, and assign it to VLAN 2000.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port access vlan 2000
```

   # Enable basic QinQ on the port.

```
[PE_A-GigabitEthernet1/0/2] qinq enable
[PE_A-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

   # Configure the port as a trunk port, and assign it to VLAN 1000 and VLAN 2000.

```
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

   # Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_A-GigabitEthernet1/0/3] quit
```

Configuring PE B

1. Create VLAN 1000 and VLAN 2000.

```
<PE_B> system-view
[PE_B] vlan 1000
[PE_B-vlan1000] quit
[PE_B] vlan 2000
[PE_B-vlan2000] quit
```

2. Configure GigabitEthernet 1/0/1 (a customer-side port):

Configure the port as a hybrid port, and set its PVID to 2000.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-GigabitEthernet1/0/1] port hybrid pvid vlan 2000
```

Assign the port to VLAN 2000 as an untagged VLAN member, and remove it from VLAN 1.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2000 untagged
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Enable basic QinQ on the port.

```
[PE_B-GigabitEthernet1/0/1] qinq enable
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

Configure the port as an access port, and assign it to VLAN 1000.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port access vlan 1000
```

Enable basic QinQ on the port.

```
[PE_B-GigabitEthernet1/0/2] qinq enable
[PE_B-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

Configure the port as a trunk port, and assign it to VLAN 1000 and VLAN 2000.

```
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_B-GigabitEthernet1/0/3] quit
```

Configuring devices in the service provider network

All ports on the path between PE A and PE B must allow frames from VLAN 1000 and VLAN 2000 to pass through without removing the VLAN tag. (Details not shown.)

Verifying the configuration

Verify the configuration on each port. For example, verify the configuration on GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
return
```

Configuration files

- PE A:

```
#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
```

- PE B:

```
#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2000 untagged
 port hybrid pvid vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
```

```
undo port trunk permit vlan 1
port trunk permit vlan 1000 2000
```

Example: Configuring selective QinQ

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 176, Customer A and Customer B each have two branches that require Layer 2 connectivity over the service provider network.

Both customers have three types of traffic and require different transmission priorities for the three types of traffic.

Configure selective QinQ on PE A and PE B to separate the traffic by customer and traffic type. Assign different 802.1p priority values to the traffic flows.

Figure 176 Network diagram

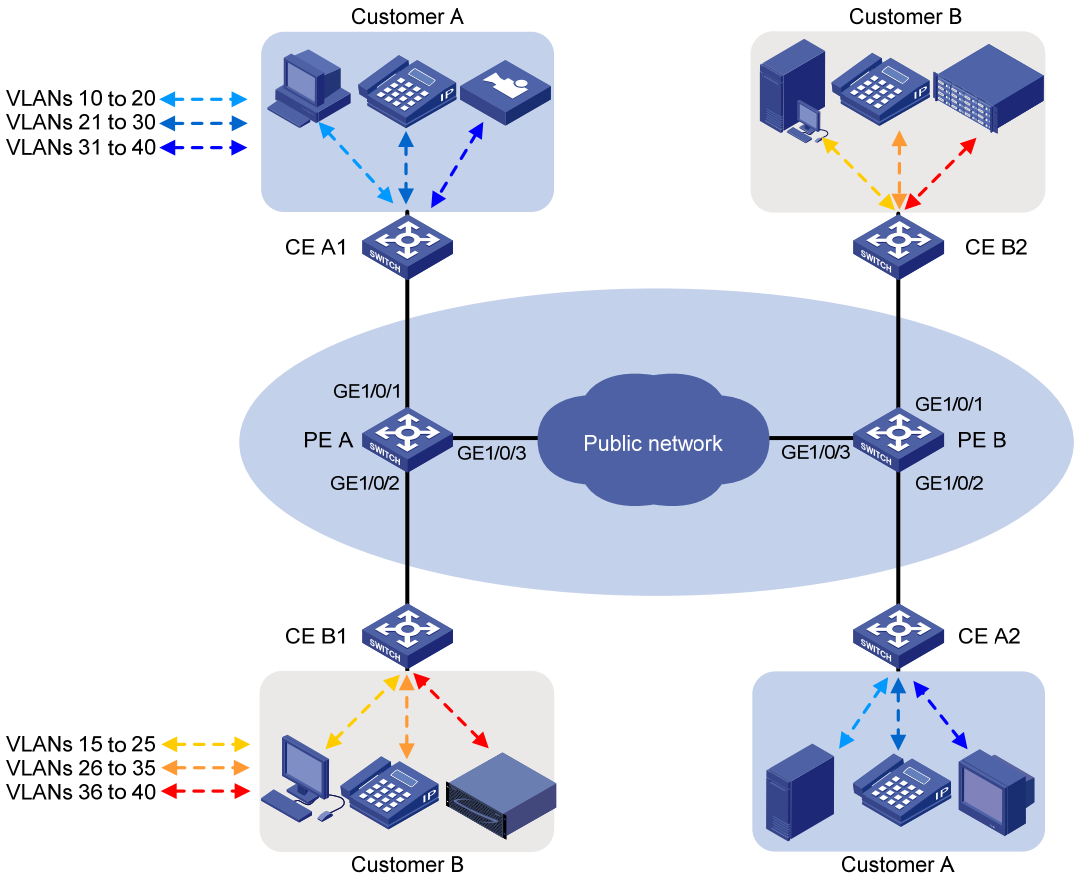
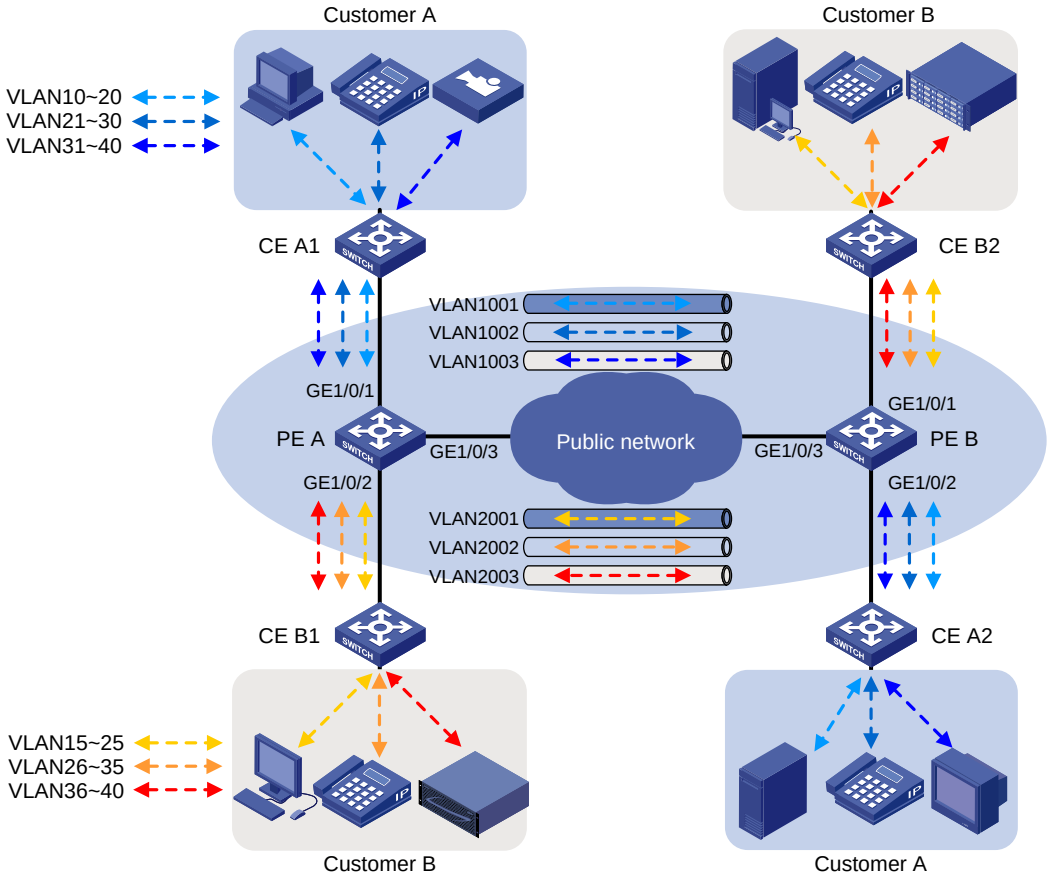


Table 21 shows the VLAN assignment scheme. For each customer, the service provider assigns one SVLAN by traffic type. Figure 177 shows the traffic transmission pattern after selective QinQ is configured.

Table 21 VLAN assignment

Traffic type	CVLANs	SVLAN	Traffic priority
Customer A:			
Video	31 to 40	1003	High
Voice	21 to 30	1002	Medium
Data	10 to 20	1001	Low
Customer B:			
Storage	36 to 40	2003	High
Voice	26 to 35	2002	Medium
Data	15 to 25	2001	Low

Figure 177 Traffic pattern in the service provider network after selective QinQ is configured



Requirements analysis

To run QinQ, you only need to configure selective QinQ on customer-side ports of PEs.

To implement selective QinQ, the customer-side ports must be hybrid ports, because they must support multiple SVLANs and must send traffic to the customer site with the SVLAN tag removed.

To send QinQ frames across the service provider network, you must configure all the ports on the forwarding path to allow frames from VLAN 1000 and VLAN 2000 to pass through without removing the VLAN tag.

Configuration restrictions and guidelines

When you configure selective QinQ, follow these restrictions and guidelines:

- You must enable basic QinQ before applying a QoS policy that contains the nest action to a port for selective QinQ.
- You can apply a QoS policy that contains the nest action to the inbound direction of ports.
- If an incoming frame does not match the selective QinQ QoS policy, the port adds the PVID tag to the frame as the SVLAN tag.
- By default, the port copies 802.1p priority from the CVLAN tag to the SVLAN tag. For untagged incoming frames, the port encapsulates the port priority as the 802.1p priority in the SVLAN tag.

- A QinQ-enabled port cannot modify the CVLAN tag. To modify CVLAN IDs, configure CVLAN ID substitution on the service provider-side port.
- Increase the MTU to at least 1504 bytes for each port on the path of QinQ frames for forwarding QinQ frames.

Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

This example assigns SVLAN tags to frames based on CVLAN IDs. You can also base SVLAN tag assignment on other criteria such as IP addresses and MAC addresses.

Configuring PE A

1. Create SVLAN 1001 through SVLAN 1003 and SVLAN 2001 through SVLAN 2003.

```
<PE_A> system-view
[PE_A] vlan 1001 to 1003
[PE_A] vlan 2001 to 2003
```

2. Configure GigabitEthernet 1/0/1 (a customer-side port):

   # Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Assign the port to SVLAN 1001 through SVLAN 1003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
```

   # Enable basic QinQ on the port.

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

   # Configure the port to trust the 802.1p priority of frames. (By default, the 802.1p priority of frames is trusted. Skip this step if you have not changed the default setting.)

```
[PE_A-GigabitEthernet1/0/1] undo qos trust
[PE_A-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

   # Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port link-type hybrid
[PE_A-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

   # Assign the port to SVLAN 2001 through SVLAN 2003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
```

   # Enable basic QinQ on the port.

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

   # Configure the port to trust the 802.1p priority of frames. (By default, the 802.1p priority of frames is trusted. Skip this step if you have not changed the default setting.)

```
[PE_A-GigabitEthernet1/0/2] undo qos trust
[PE_A-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

   # Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/3
```

```
[PE_A-GigabitEthernet1/0/3] port link-type trunk
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLAN 1001 through SVLAN 1003 and SVLAN 2001 through SVLAN 2003.

```
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_A-GigabitEthernet1/0/3] quit
```

5. Configure a QoS policy:

Create a class named **customer_A_pc** to match traffic from CVLAN 10 through CVLAN 20 (data traffic) for Customer A.

```
[PE_A] traffic classifier customer_A_pc
[PE_A-classifier-customer_A_pc] if-match customer-vlan-id 10 to 20
[PE_A-classifier-customer_A_pc] quit
```

Create the classes **customer_A_voice** and **customer_A_video** to match Customer A's voice traffic and video traffic, respectively.

```
[PE_A] traffic classifier customer_A_voice
[PE_A-classifier-customer_A_voice] if-match customer-vlan-id 21 to 30
[PE_A-classifier-customer_A_voice] quit
[PE_A] traffic classifier customer_A_video
[PE_A-classifier-customer_A_video] if-match customer-vlan-id 31 to 40
[PE_A-classifier-customer_A_video] quit
```

Configure SVLAN tagging behaviors for Customer A's three traffic types. Replace the 802.1p priority in the SVLAN tags of matching frames with the configured priority.

```
[PE_A] traffic behavior customer_A_pc
[PE_A-behavior-customer_A_pc] nest top-most vlan-id 1001
[PE_A-behavior-customer_A_pc] remark dot1p 3
[PE_A-behavior-customer_A_pc] quit
[PE_A] traffic behavior customer_A_voice
[PE_A-behavior-customer_A_voice] nest top-most vlan-id 1002
[PE_A-behavior-customer_A_voice] remark dot1p 5
[PE_A-behavior-customer_A_voice] quit
[PE_A] traffic behavior customer_A_video
[PE_A-behavior-customer_A_video] nest top-most vlan-id 1003
[PE_A-behavior-customer_A_video] remark dot1p 7
[PE_A-behavior-customer_A_video] quit
```

Create a QoS policy named **customer_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_A] qos policy customer_A
[PE_A-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_A-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_A-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_A-qospolicy-customer_A] quit
```

Apply the QoS policy **customer_A** to the inbound direction of GigabitEthernet 1/0/1.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] qos apply policy customer_A inbound
[PE_A-GigabitEthernet1/0/1] quit
```

Create traffic classes for matching Customer B's three traffic types.

```
[PE_A] traffic classifier customer_B_pc
[PE_A-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
```

```
[PE_A-classifier-customer_B_pc] quit
[PE_A] traffic classifier customer_B_voice
[PE_A-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_A-classifier-customer_B_voice] quit
[PE_A] traffic classifier customer_B_storage
[PE_A-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_A-classifier-customer_B_storage] quit
```

Configure SVLAN tagging behaviors for Customer B's traffic types. Replace the 802.1p priority in the SVLAN tags of matching frames with the configured priority.

```
[PE_A] traffic behavior customer_B_pc
[PE_A-behavior-customer_B_pc] nest top-most vlan-id 2001
[PE_A-behavior-customer_B_pc] remark dot1p 3
[PE_A-behavior-customer_B_pc] quit
[PE_A] traffic behavior customer_B_voice
[PE_A-behavior-customer_B_voice] nest top-most vlan-id 2002
[PE_A-behavior-customer_B_voice] remark dot1p 5
[PE_A-behavior-customer_B_voice] quit
[PE_A] traffic behavior customer_B_storage
[PE_A-behavior-customer_B_storage] nest top-most vlan-id 2003
[PE_A-behavior-customer_B_storage] remark dot1p 7
[PE_A-behavior-customer_B_storage] quit
```

Create a QoS policy named **customer_B** for Customer B, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_A] qos policy customer_B
[PE_A-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_A-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_A-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_A-qospolicy-customer_B] quit
```

Apply the QoS policy **customer_B** to the inbound direction of GigabitEthernet 1/0/2.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] qos apply policy customer_B inbound
[PE_A-GigabitEthernet1/0/2] quit
```

Configuring PE B

1. Create SVLAN 1001 through SVLAN 1003 and SVLAN 2001 through SVLAN 2003.

```
<PE_B> system-view
[PE_B] vlan 1001 to 1003
[PE_B] vlan 2001 to 2003
```

2. Configure GigabitEthernet 1/0/1 (a customer-side port):

Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Assign the port to SVLAN 2001 through SVLAN 2003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

Enable basic QinQ on the port.

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

Configure the port to trust the 802.1p priority of frames. (By default, the 802.1p priority of frames is trusted. Skip this step if you have not changed the default setting.)

```
[PE_B-GigabitEthernet1/0/1] undo qos trust
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port link-type hybrid
[PE_B-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Assign the port to SVLAN 1001 through SVLAN 1003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
```

Enable basic QinQ on the port.

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

Configure the port to trust the 802.1p priority of frames. (By default, the 802.1p priority of frames is trusted. Skip this step if you have not changed the default setting.)

```
[PE_B-GigabitEthernet1/0/2] undo qos trust
[PE_B-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLAN 1001 through SVLAN 1003 and SVLAN 2001 through SVLAN 2003.

```
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-GigabitEthernet1/0/3] quit
```

5. Configure a QoS policy:

#Create traffic classes for matching Customer A's traffic types.

```
[PE_B] traffic classifier customer_A_pc
[PE_B-classifier-customer_A_pc] if-match customer-vlan-id 10 to 20
[PE_B-classifier-customer_A_pc] quit
[PE_B] traffic classifier customer_A_voice
[PE_B-classifier-customer_A_voice] if-match customer-vlan-id 21 to 30
[PE_B-classifier-customer_A_voice] quit
[PE_B] traffic classifier customer_A_video
[PE_B-classifier-customer_A_video] if-match customer-vlan-id 31 to 40
[PE_B-classifier-customer_A_video] quit
```

Configure SVLAN tagging behaviors for Customer A's three traffic types. Replace the 802.1p priority in the SVLAN tags of matching frames with the configured priority.

```
[PE_B] traffic behavior customer_A_pc
[PE_B-behavior-customer_A_pc] nest top-most vlan-id 1001
[PE_B-behavior-customer_A_pc] remark dot1p 3
[PE_B-behavior-customer_A_pc] quit
[PE_B] traffic behavior customer_A_voice
[PE_B-behavior-customer_A_voice] nest top-most vlan-id 1002
[PE_B-behavior-customer_A_voice] remark dot1p 5
```

```
[PE_B-behavior-customer_A_voice] quit
[PE_B] traffic behavior customer_A_video
[PE_B-behavior-customer_A_video] nest top-most vlan-id 1003
[PE_B-behavior-customer_A_video] remark dot1p 7
[PE_B-behavior-customer_A_video] quit
```

Create a QoS policy named **customer_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_B] qos policy customer_A
[PE_B-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_B-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_B-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_B-qospolicy-customer_A] quit
```

Apply QoS policy **customer_A** to the inbound direction of GigabitEthernet 1/0/2.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] qos apply policy customer_A inbound
[PE_B-GigabitEthernet1/0/2] quit
```

Create traffic classes for matching Customer B's three traffic types.

```
[PE_B] traffic classifier customer_B_pc
[PE_B-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_B-classifier-customer_B_pc] quit
[PE_B] traffic classifier customer_B_voice
[PE_B-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_B-classifier-customer_B_voice] quit
[PE_B] traffic classifier customer_B_storage
[PE_B-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_B-classifier-customer_B_storage] quit
```

Configure SVLAN tagging behaviors for Customer B's three traffic types. Replace the 802.1p priority in the SVLAN tags of matching frames with the configured priority.

```
[PE_B] traffic behavior customer_B_pc
[PE_B-behavior-customer_B_pc] nest top-most vlan-id 2001
[PE_B-behavior-customer_B_pc] remark dot1p 3
[PE_B-behavior-customer_B_pc] quit
[PE_B] traffic behavior customer_B_voice
[PE_B-behavior-customer_B_voice] nest top-most vlan-id 2002
[PE_B-behavior-customer_B_voice] remark dot1p 5
[PE_B-behavior-customer_B_voice] quit
[PE_B] traffic behavior customer_B_storage
[PE_B-behavior-customer_B_storage] nest top-most vlan-id 2003
[PE_B-behavior-customer_B_storage] remark dot1p 7
[PE_B-behavior-customer_B_storage] quit
```

Create a QoS policy named **customer_B** for Customer B, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_B] qos policy customer_B
[PE_B-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_B-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_B-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_B-qospolicy-customer_B] quit
```

Apply the QoS policy **customer_B** to the inbound direction of GigabitEthernet 1/0/1.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] qos apply policy customer_B inbound
[PE_B-GigabitEthernet1/0/1] quit
```

Configuring devices in the service provider network

All ports on the path between PE A and PE B must allow frames from VLAN 1001 through VLAN 1003 and VLAN 2001 through VLAN 2003 to pass through without removing the VLAN tag. (Details not shown.)

Verifying the configuration

Use the **display this** command to verify the configuration on each port, for example, on GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos apply policy customer_A inbound
#
Return
[PE_A-GigabitEthernet1/0/1] quit
```

Use the **display qos policy interface** command to verify the QoS configuration on each port, for example, on GigabitEthernet 1/0/1 of PE A.

```
[PE_A] display qos policy interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: customer_A
   Classifier: customer_A_pc
     Operator: AND
     Rule(s) : If-match customer-vlan-id 10 to 20
     Behavior: customer_A_pc
      Nesting:
        Nest top-most vlan-id 1001
      Marking:
        Remark dot1p COS 3
   Classifier: customer_A_voice
     Operator: AND
     Rule(s) : If-match customer-vlan-id 21 to 30
     Behavior: customer_A_voice
      Nesting:
```

```
    Nest top-most vlan-id 1002
   Marking:
    Remark dot1p COS 5
Classifier: customer_A_video
  Operator: AND
  Rule(s) : If-match customer-vlan-id 31 to 40
  Behavior: customer_A_video
   Nesting:
    Nest top-most vlan-id 1003
   Marking:
    Remark dot1p COS 7
```

Configuration files

- PE A:

```
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
 if-match customer-vlan-id 10 to 20
traffic classifier customer_A_voice operator and
 if-match customer-vlan-id 21 to 30
traffic classifier customer_A_video operator and
 if-match customer-vlan-id 31 to 40
traffic classifier customer_B_pc operator and
 if-match customer-vlan-id 15 to 25
traffic classifier customer_B_voice operator and
 if-match customer-vlan-id 26 to 35
traffic classifier customer_B_storage operator and
 if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
 nest top-most vlan-id 1001
 remark dot1p 3
traffic behavior customer_A_voice
 nest top-most vlan-id 1002
 remark dot1p 5
traffic behavior customer_A_video
 nest top-most vlan-id 1003
 remark dot1p 7
traffic behavior customer_B_pc
 nest top-most vlan-id 2001
 remark dot1p 3
traffic behavior customer_B_voice
 nest top-most vlan-id 2002
 remark dot1p 5
```

```
traffic behavior customer_B_storage
 nest top-most vlan-id 2003
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc
 classifier customer_B_voice behavior customer_B_voice
 classifier customer_B_storage behavior customer_B_storage

interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
 qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
```

- PE B:

```
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
 if-match customer-vlan-id 10 to 20
traffic classifier customer_A_voice operator and
 if-match customer-vlan-id 21 to 30
traffic classifier customer_A_video operator and
 if-match customer-vlan-id 31 to 40
traffic classifier customer_B_pc operator and
 if-match customer-vlan-id 15 to 25
```

```
traffic classifier customer_B_voice operator and
 if-match customer-vlan-id 26 to 35
traffic classifier customer_B_storage operator and
 if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
 nest top-most vlan-id 1001
 remark dot1p 3
traffic behavior customer_A_voice
 nest top-most vlan-id 1002
 remark dot1p 5
traffic behavior customer_A_video
 nest top-most vlan-id 1003
 remark dot1p 7
traffic behavior customer_B_pc
 nest top-most vlan-id 2001
 remark dot1p 3
traffic behavior customer_B_voice
 nest top-most vlan-id 2002
 remark dot1p 5
traffic behavior customer_B_storage
 nest top-most vlan-id 2003
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc
 classifier customer_B_voice behavior customer_B_voice
 classifier customer_B_storage behavior customer_B_storage

interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
 qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos apply policy customer_A inbound
```

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
```

Example: Changing the CVLAN TPID and the SVLAN TPID

TPID identifies a frame as an 802.1Q tagged frame. By default, the switch sets the TPID in 802.1Q VLAN tags to 0x8100 and identifies frames that carry 0x8100 as tagged. This value might differ by vendor. For 802.1Q tagged frames to be identified correctly in a multi-vendor network, you must set the TPID setting on one vendor's device to be compatible with another vendor's device.

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

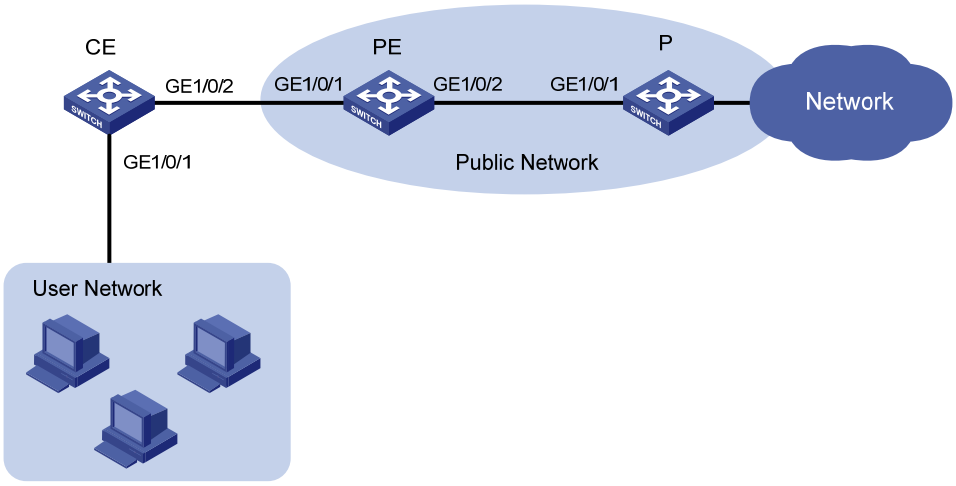
Network requirements

As shown in Figure 178, basic QinQ is enabled on GigabitEthernet 1/0/1 of the PE.

The TPID in the 802.1Q-tagged frames from the CE is 0x8200. The TPID in the 802.1Q-tagged frames from the P device is 0x9100.

Change the CVLAN TPID and SVLAN TPID on the PE to be compatible with the CE and the P device.

Figure 178 Network diagram



Requirements analysis

The switch supports one global CVLAN PVID for all QinQ-enabled ports. On a port with basic QinQ enabled, the switch identifies VLAN tagged frames based on the global CVLAN TPID. However, the switch does not change the TPID in CVLAN tags. An incoming frame is handled as an untagged frame if its TPID is different from the global CVLAN TPID.

If you are implementing selective QinQ, you must make sure the CVLAN TPID on the switch is the same as the VLAN TPID on the customer device, because incorrect identification of frames can result in an SVLAN assignment mistake. If you are implementing basic QinQ, you do not need to change the CVLAN TPID because CVLAN TPID mismatch does not affect SVLAN assignment.

For the PE in this example to identify CVLAN-tagged frames correctly on GigabitEthernet 1/0/1, you must change the global CVLAN TPID to 0x8200.

SVLAN TPIDs are configurable on a per-port basis. A service provider-side port uses the SVLAN TPID to re-mark the TPID in outgoing frames' SVLAN tags, in addition to matching incoming tagged frames.

For the P device and the PE in this example to handle 802.1Q tagged frames correctly, you must change the SVLAN TPID to 0x9100 on GigabitEthernet 1/0/2 of the PE.

Configuration restrictions and guidelines

When you configure TPID, follow these restrictions and guidelines:

- Configure the SVLAN TPID on the service provider-side ports. You cannot configure the SVLAN TPID on QinQ-enabled ports.
- Increase the MTU to at least 1504 bytes for each port on the path of QinQ frames for forwarding QinQ frames.

Configuration procedures

1. Create VLAN 1000 on the PE. This example uses VLAN 1000 as an SVLAN.

```
<PE> system-view
[PE] vlan 1000
[PE-vlan1000] quit
```

2. Globally set the CVLAN TPID to 0x8200.

```
[PE] qinq ethernet-type customer-tag 8200
```

3. Configure GigabitEthernet 1/0/1 (the customer-side port):

   # Configure the port as a hybrid port, set its PVID to 1000, and remove it from VLAN 1.

```
[PE] interface gigabitethernet 1/0/1
[PE-GigabitEthernet1/0/1] port link-type hybrid
[PE-GigabitEthernet1/0/1] port hybrid pvid vlan 1000
[PE-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Assign the port to VLAN 1000 as an untagged VLAN member.

```
[PE-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

   # Enable basic QinQ on GigabitEthernet 1/0/1.

```
[PE-GigabitEthernet1/0/1] qinq enable
[PE-GigabitEthernet1/0/1] quit
```

4. Configure GigabitEthernet 1/0/2 (the service-provider-side port):

Configure the port as a trunk port, assign it to VLAN 1000, and remove it from VLAN 1.

```
[PE] interface gigabitethernet 1/0/2
[PE-GigabitEthernet1/0/2] port link-type trunk
[PE-GigabitEthernet1/0/2] port trunk permit vlan 1000
[PE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

Set the SVLAN TPID to 0x9100 on the port.

```
[PE-GigabitEthernet1/0/2] qinq ethernet-type service-tag 9100
[PE-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Use the **display current-configuration | include qinq ethernet-type customer-tag** command to verify the CVLAN TPID setting.

```
[PE] display current-configuration | include qinq ethernet-type customer-tag
 qinq ethernet-type customer-tag 8200
```

Use the **display this** command to verify the SVLAN TPID setting.

```
[PE] interface gigabitethernet 1/0/2
[PE-GigabitEthernet1/0/2] display this
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000
 qinq ethernet-type service-tag 9100
#
return
```

NOTE:

No commands are available to display the initial settings. If the default TPID is 0x8100 (the initial setting), the **display current-configuration** and **display this** commands do not display the TPID setting.

Configuration files

```
#
qinq ethernet-type customer-tag 8200
#
vlan 1000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000
 qinq ethernet-type service-tag 9100
```

Traffic policing configuration examples

This chapter provides examples for configuring traffic policing and aggregation CAR to control network traffic.

Example: Policing traffic by IP address and protocol

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

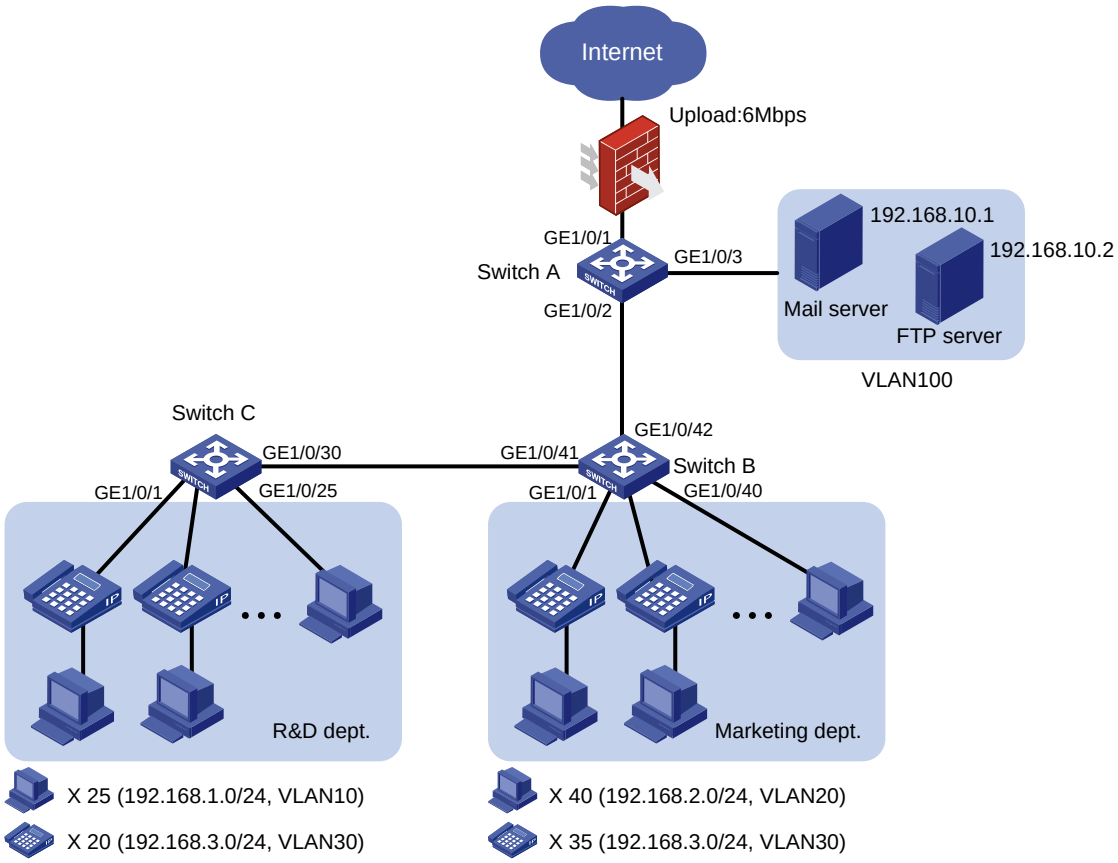
Network requirements

As shown in Figure 179, a company uses a dedicated line to access the Internet, with an uplink bandwidth of 6 Mbps. All end devices use the firewall as the gateway.

Configure traffic policing to classify and rate limit the upstream traffic as follows:

- **HTTP traffic**—Rate limit HTTP traffic to a total of 3 Mbps. 1 Mbps is for the 25 hosts in the R & D department, and each host is limited to a maximum of 128 kbps. 2 Mbps is for the 40 hosts in the Marketing department, and each host is limited to a maximum of 256 kbps.
- **VoIP traffic**—Rate limit VoIP traffic to 640 kbps for the 55 IP phones in the two departments. An IP phone requires 32 kbps when in conversation. 640 kbps supports 20 IP phones that are in calls simultaneously. To accommodate more IP phones, a peak rate of 800 kbps is allowed.
- **Email traffic**—A mail server forwards emails for all clients to the external network. Rate limit email traffic to 512 kbps.
- **FTP traffic**—An FTP server provides data services for the branches through the external network. Rate limit email traffic to 1 Mbps.

Figure 179 Network diagram



Requirements analysis

Configure ACLs to classify packets of different traffic types.

Associate classes of packets with policing actions to rate limit different traffic types.

Configuration restrictions and guidelines

In a traffic behavior, the traffic policing action cannot be configured together with a priority marking action (local precedence, drop precedence, 802.1p priority, DSCP, or IP precedence marking). Otherwise, a QoS policy that references such a behavior cannot be applied correctly.

Configuration procedures

Configuring Switch A

1. Configure VLAN attributes for the interfaces:

   # Configure GigabitEthernet 1/0/1 as a trunk port.

   ```
   <SwitchA> system-view
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-type trunk
   ```

   # Assign the port to VLAN 10, VLAN 20, VLAN 30, and VLAN 100.

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 10 20 30 100
```

Remove the port from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLAN 10, VLAN 20, and VLAN 30.

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 10 20 30
```

Remove the port from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as an access port.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/3
```

Assign the port to VLAN 100.

```
[SwitchA-GigabitEthernet1/0/3] port access vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

2. Configure traffic classes and behaviors for HTTP traffic:

Create advanced IPv4 ACL 3000 to match the HTTP traffic from the R & D department.

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.0
0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Create a class named **rd_http**, and use advanced IPv4 ACL 3000 as the match criterion.

```
[SwitchA] traffic classifier rd_http
[SwitchA-classifier-rd_http] if-match acl 3000
[SwitchA-classifier-rd_http] quit
```

Create a behavior named **rd_http**, and configure traffic policing: CIR 1024 kbps and CBS 6225 bytes.

```
[SwitchA] traffic behavior rd_http
[SwitchA-behavior-rd_http] car cir 1024 cbs 6225
[SwitchA-behavior-rd_http] quit
```

Create advanced IPv4 ACL 3001 to match the HTTP traffic from the Marketing department.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit tcp destination-port eq 80 source 192.168.2.0
0.0.0.255
[SwitchA-acl-adv-3001] quit
```

Create a class named **mkt_http**, and use advanced IPv4 ACL 3001 as the match criterion.

```
[SwitchA] traffic classifier mkt_http
[SwitchA-classifier-mkt_http] if-match acl 3001
[SwitchA-classifier-mkt_http] quit
```

Create a behavior named **mkt_http**, and configure traffic policing: CIR 2048 kbps and CBS 13108 bytes.

```
[SwitchA] traffic behavior mkt_http
[SwitchA-behavior-mkt_http] car cir 2048 cbs 13108
```

```
[SwitchA-behavior-mkt_http] quit
```

3. Configure traffic classes and behaviors for VoIP traffic:

   # Create basic IPv4 ACL 2000 to match the VoIP traffic.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 192.168.3.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

   # Create a class named **ip_voip**, and use basic IPv4 ACL 2000 as the match criterion.

```
[SwitchA] traffic classifier ip_voip
[SwitchA-classifier-ip_voip] if-match acl 2000
[SwitchA-classifier-ip_voip] quit
```

   # Create a behavior named **ip_voip**, and configure traffic policing: CIR 640 kbps, CBS 4096 bytes, EBS 1024 bytes, and PIR 800 kbps.

```
[SwitchA] traffic behavior ip_voip
[SwitchA-behavior-ip_voip] car cir 640 cbs 4096 ebs 1024 pir 800
[SwitchA-behavior-ip_voip] quit
```

4. Configure traffic classes and behaviors for email traffic:

   # Create advanced IPv4 ACL 3002 to match the email traffic.

```
[SwitchA] acl number 3002
[SwitchA-acl-adv-3002] rule permit tcp destination-port eq smtp source 192.168.10.1
0.0.0.0
[SwitchA-acl-adv-3002] quit
```

   # Create a class named **email**, and use advanced IPv4 ACL 3002 as the match criterion.

```
[SwitchA] traffic classifier email
[SwitchA-classifier-email] if-match acl 3002
[SwitchA-classifier-email] quit
```

   # Create a behavior named **email**, and configure traffic policing: CIR 512 kbps and CBS 3277 bytes.

```
[SwitchA] traffic behavior email
[SwitchA-behavior-email] car cir 512 cbs 3277
[SwitchA-behavior-email] quit
```

5. Configure traffic classes and behaviors for FTP traffic:

   # Create basic IPv4 ACL 2001 to match the FTP traffic.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 192.168.10.2 0.0.0.0
[SwitchA-acl-basic-2001] quit
```

   # Create a class named **ftp**, and use advanced IPv4 ACL 2001 as the match criterion.

```
[SwitchA] traffic classifier ftp
[SwitchA-classifier-ftp] if-match acl 2001
[SwitchA-classifier-ftp] quit
```

   # Create a behavior named **ftp**, and configure traffic policing: CIR 1024 kbps and CBS 6554 bytes.

```
[SwitchA] traffic behavior ftp
[SwitchA-behavior-ftp] car cir 1024 cbs 6554
[SwitchA-behavior-ftp] quit
```

6. Configure QoS policies and apply them to interfaces:

   # Create a QoS policy named **http&voice**.

```
[SwitchA] qos policy http&voice
```

Associate the classes **rd_http**, **mkt_http**, and **ip_voip** with the behaviors **rd_http**, **mkt_http**, and **ip_voip** in **http&voice**, respectively.

```
[SwitchA-qospolicy-http&voice] classifier rd_http behavior rd_http
[SwitchA-qospolicy-http&voice] classifier mkt_http behavior mkt_http
[SwitchA-qospolicy-http&voice] classifier ip_voip behavior ip_voip
[SwitchA-qospolicy-http&voice] quit
```

Apply the QoS policy **http&voice** to the inbound direction of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy http&voice inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Create a QoS policy named **email&ftp**.

```
[SwitchA] qos policy email&ftp
```

Associate the classes **email** and **ftp** with the behaviors **email** and **ftp** in **email&ftp**, respectively.

```
[SwitchA-qospolicy-email&ftp] classifier email behavior email
[SwitchA-qospolicy-email&ftp] classifier ftp behavior ftp
[SwitchA-qospolicy-email&ftp] quit
```

Apply the QoS policy **email&ftp** to the inbound direction of GigabitEthernet 1/0/3.

```
[SwitchA] interface GigabitEthernet1/0/3
[SwitchA- GigabitEthernet1/0/3] port link-mode bridge
[SwitchA- GigabitEthernet1/0/3] qos apply policy email&ftp inbound
```

Configuring Switch B

In this example, the IP phones support sending VLAN-tagged voice packets. For information about how IP phones obtain VLAN information, see the configuration guide for the switch.

If the switch is configured with the auto-mode voice VLAN function, the interfaces connecting to IP phones do not need to be assigned to VLAN 30.

1. Configure interfaces and VLANs:

Create port group 1.

```
<SwitchB> system-view
[SwitchB] port-group manual 1
```

Add all interfaces that connect to hosts and IP phones to port group 1.

```
[SwitchB-port-group-manual-1] group-member GigabitEthernet 1/0/1 to GigabitEthernet
1/0/40
```

Configure the interfaces in port group 1 as trunk ports.

```
[SwitchB-port-group-manual-1] port link-type trunk
```

Configure the PVID of these interfaces as VLAN 20.

```
[SwitchB-port-group-manual-1] port trunk pvid vlan 20
```

Assign these interfaces to VLAN 20 and VLAN 30, and remove these interfaces from VLAN 1.

```
[SwitchB-port-group-manual-1] port trunk permit vlan 20 30
[SwitchB-port-group-manual-1] undo port trunk permit vlan 1
[SwitchB-port-group-manual-1] quit
```

Configure GigabitEthernet 1/0/41 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/41
[SwitchB-GigabitEthernet1/0/41] port link-type trunk
```

Assign GigabitEthernet 1/0/41 to VLAN 10 and VLAN 30, and remove it from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/41] port trunk permit vlan 10 30
[SwitchB-GigabitEthernet1/0/41] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/41] quit
```

Configure GigabitEthernet 1/0/42 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/42
[SwitchB-GigabitEthernet1/0/42] port link-type trunk
```

Assign it to VLAN 10, VLAN 20, and VLAN 30, and remove it from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/42] port trunk permit vlan 10 20 30
[SwitchB-GigabitEthernet1/0/42] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/42] quit
```

2. Configure traffic policing:

Create advanced IPv4 ACL 3000 to match the HTTP traffic from the Marketing department.

```
[SwitchB] acl number 3000
[SwitchB-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.2.0
0.0.0.255
[SwitchB-acl-adv-3000] quit
```

Create a class named **mkt**, and use advanced IPv4 ACL 3000 as the match criterion.

```
[SwitchB] traffic classifier mkt
[SwitchB-classifier-mkt] if-match acl 3000
[SwitchB-classifier-mkt] quit
```

Create a behavior named **mkt**, and configure traffic policing: CIR 256 kbps and CBS 1638 bytes.

```
[SwitchB] traffic behavior mkt
[SwitchB-behavior-mkt] car cir 256 cbs 1638
[SwitchB-behavior-mkt] quit
```

Create a QoS policy named **mkt**, and associate the class **mkt** with the behavior **mkt** in **mkt**.

```
[SwitchB] qos policy mkt
[SwitchB-qospolicy-mkt] classifier mkt behavior mkt
```

Apply the QoS policy **mkt** to the inbound direction of port group 1.

```
[SwitchB] port-group manual 1
[SwitchB-port-group-manual-1] qos apply policy mkt inbound
```

Configuring Switch C

1. Configure interfaces and VLANs:

Create port group 1.

```
<SwitchC> system-view
[SwitchC] port-group manual 1
```

Add all interfaces that connect to hosts and IP phones to port group 1.

```
[SwitchC-port-group-manual-1] group-member GigabitEthernet 1/0/1 to GigabitEthernet
1/0/25
```

Configure the interfaces in port group 1 as trunk ports.

```
[SwitchC-port-group-manual-1] port link-type trunk
```

Configure the PVID of these interfaces as VLAN 10.

```
[SwitchC-port-group-manual-1] port trunk pvid vlan 10
```

Assign these interfaces to VLAN 10 and VLAN 30, and remove these interfaces from VLAN 1.

```
[SwitchC-port-group-manual-1] port trunk permit vlan 10 30
```

```
[SwitchC-port-group-manual-1] undo port trunk permit vlan 1
[SwitchC-port-group-manual-1] quit
```

Configure GigabitEthernet 1/0/30 as a trunk port.

```
[SwitchC] interface gigabitethernet 1/0/30
[SwitchC-GigabitEthernet1/0/30] port link-type trunk
[SwitchC-GigabitEthernet1/0/30] port trunk permit vlan 10 30
```

Assign it to VLAN 10 and VLAN 30, and remove it from VLAN 1.

```
[SwitchC-GigabitEthernet1/0/30] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/30] quit
```

2. Configure traffic policing:

Create advanced IPv4 ACL 3000 to match the HTTP traffic from the R&D department.

```
[SwitchC] acl number 3000
[SwitchC-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.0
0.0.0.255
[SwitchC-acl-adv-3000] quit
```

Create a class named **rd**, and use advanced IPv4 ACL 3000 as the match criterion.

```
[SwitchC] traffic classifier rd
[SwitchC-classifier-rd] if-match acl 3000
[SwitchC-classifier-rd] quit
```

Create a behavior named **rd**, and configure traffic policing: CIR 128 kbps and CBS 820 bytes.

```
[SwitchC] traffic behavior rd
[SwitchC-behavior-rd] car cir 128 cbs 820
[SwitchC-behavior-rd] quit
```

Create a QoS policy named **rd**, and associate the class **rd** with the behavior **rd** in the QoS policy **rd**.

```
[SwitchC] qos policy rd
[SwitchC-qospolicy-rd] classifier rd behavior rd
```

Apply the QoS policy **rd** to the inbound direction of port group 1.

```
[SwitchC] port-group manual 1
[SwitchC-port-group-manual-1] qos apply policy rd inbound
```

Configuration files

- Switch A:

```
#
acl number 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
acl number 2001
 rule 0 permit source 192.168.10.2 0
#
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
acl number 3002
 rule 0 permit tcp source 192.168.10.1 0 destination-port eq smtp
#
```

```
traffic classifier email operator and
 if-match acl 3002
traffic classifier ip_voip operator and
 if-match acl 2000
traffic classifier ftp operator and
 if-match acl 2001
traffic classifier rd_http operator and
 if-match acl 3000
traffic classifier mkt_http operator and
 if-match acl 3001
#
traffic behavior email
 car cir 512 cbs 3277 ebs 512 green pass red discard yellow pass
traffic behavior ip_voip
 car cir 640 cbs 4096 ebs 1024 pir 800 green pass red discard yellow pass
traffic behavior ftp
 car cir 1024 cbs 6554 ebs 512 green pass red discard yellow pass
traffic behavior rd_http
 car cir 1024 cbs 6554 ebs 512 green pass red discard yellow pass
traffic behavior mkt_http
 car cir 2048 cbs 13108 ebs 512 green pass red discard yellow pass
#
qos policy email&ftp
 classifier email behavior email
 classifier ftp behavior ftp
qos policy http&voice
 classifier rd_http behavior rd_http
 classifier mkt_http behavior mkt_http
 classifier ip_voip behavior ip_voip
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
 qos apply policy http&voice inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 qos apply policy email&ftp inbound
```

- Switch B:

```
#
acl number 3000
 rule 0 permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
#
traffic classifier mkt operator and
 if-match acl 3000
#
traffic behavior mkt
 car cir 256 cbs 1638 ebs 512 green pass red discard yellow pass
#
qos policy mkt
 classifier mkt behavior mkt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 port trunk pvid vlan 20
 qos apply policy mkt inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 port trunk pvid vlan 20
 qos apply policy mkt inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 port trunk pvid vlan 20
 qos apply policy mkt inbound
…
#
interface GigabitEthernet1/0/41
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 30
 qos apply policy mkt inbound
#
interface GigabitEthernet1/0/42
 port link-mode bridge
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
 qos apply policy mkt inbound
```

- Switch C:

```
#
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq www
#
traffic classifier rd operator and
 if-match acl 3000
#
traffic behavior rd
 car cir 128 cbs 820 ebs 512 green pass red discard yellow pass
#
qos policy rd
 classifier rd behavior rd
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 30
 port trunk pvid vlan 10
 qos apply policy rd inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 30
 port trunk pvid vlan 10
 qos apply policy rd inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 30
 port trunk pvid vlan 10
 qos apply policy rd inbound
…
#
interface GigabitEthernet1/0/30
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 30
```

Example: Policing traffic by VLAN-based bandwidth allocation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

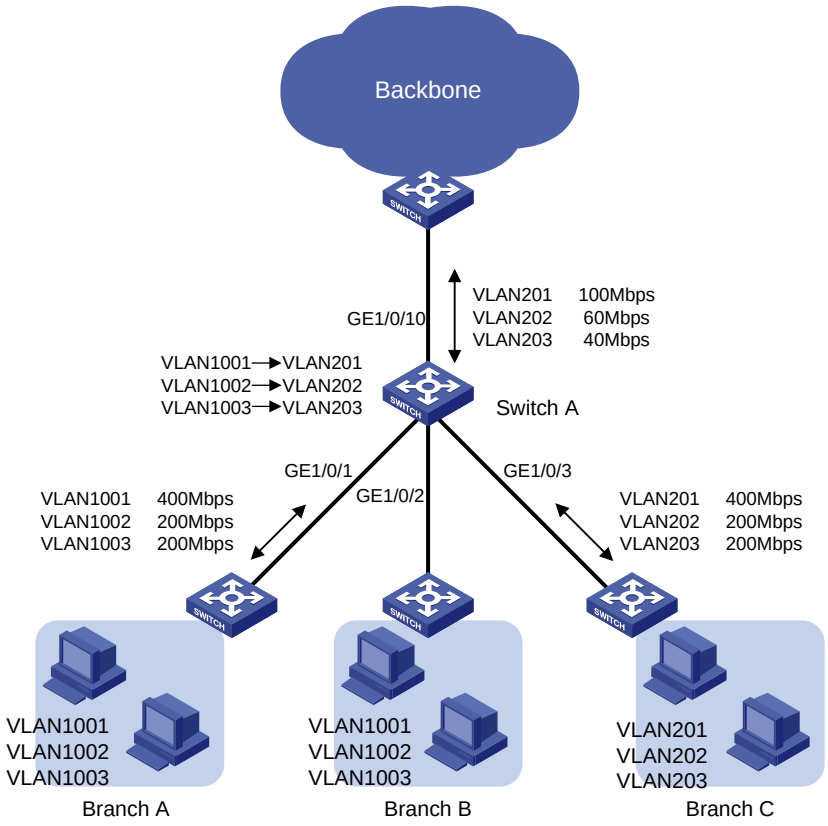
As shown in Figure 180, Switch A aggregates traffic from the branches and transmits the traffic to the backbone network through a leased line. Each branch site assigns packets to different VLANs based on applications.

Configure one-to-one VLAN mapping on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A to re-map traffic of different applications to VLANs as per the transmission scheme on the backbone network.

Configure traffic policing to allocate bandwidth to traffic from different VLANs, as follows:

- On the links connecting to Branch A and Branch B, limit the upstream rate to 400 Mbps for traffic of VLAN 1001, 200 Mbps for VLAN 1002, and 200 Mbps for VLAN 1003. The same settings apply to the downstream traffic to the branches over the two links.
- On the link connecting to Branch C, limit the upstream rate to 400 Mbps for traffic of VLAN 201, 200 Mbps for VLAN 202, and 200 Mbps for VLAN 203. The same settings apply to the downstream traffic to Branch C over the link.
- On the link connecting to the backbone network, limit the upstream rate to 100 Mbps for traffic of VLAN 201, 60 Mbps for VLAN 202, and 40 Mbps for VLAN 203. The same settings apply to the downstream traffic from the backbone network to Switch A over the link.

Figure 180 Network diagram



Requirements analysis

To allocate bandwidth based on VLANs, you need to use QoS policies. This involves the following:

- Configuring VLAN-based traffic classes.
- Configuring per-VLAN traffic policing behaviors.
- Associating each class with its specific traffic behavior.

VLAN mapping is also implemented with QoS policies. When VLAN mapping is involved, be careful with the order you reference the VLAN mapping and policing actions in the QoS policy and the target traffic class to be policed.

If the VLAN mapping action is referenced first, the device marks the traffic with the new VLAN ID and looks up the QoS policy based on the new VLAN ID. If the policing action is associated with the class for the original VLAN, this renders the policing action useless for the traffic. Likewise, associating the policing action with the class for the original VLAN first renders the VLAN mapping action useless. This is because the device stops searching the QoS policy once a match is found.

Configuration restrictions and guidelines

When you configure traffic policing by VLAN-based bandwidth allocation, follow these restrictions and guidelines:

- QinQ must be enabled before a QoS policy is applied. You cannot enable QinQ on a port if a QoS policy has been applied the port.

- In a traffic behavior, the traffic policing action cannot be configured together with a priority marking action (local precedence, drop precedence, 802.1p priority, DSCP, or IP precedence marking). Otherwise, a QoS policy that references such a behavior cannot be applied correctly.

Configuration procedures

Configuring bandwidth allocation unrelated to VLAN mapping

Create a class named **vlan201**, and configure SVLAN 201 as the match criterion.

```
<SwitchA> system-view
[SwitchA] traffic classifier vlan201
[SwitchA-classifier-vlan201] if-match service-vlan-id 201
[SwitchA-classifier-vlan201] quit
```

Create classes named **vlan202** and **vlan203**, and configure SVLAN 202 and SVLAN 203 as their match criteria, respectively.

```
[SwitchA] traffic classifier vlan202
[SwitchA-classifier-vlan202] if-match service-vlan-id 202
[SwitchA-classifier-vlan202] quit
[SwitchA] traffic classifier vlan203
[SwitchA-classifier-vlan203] if-match service-vlan-id 203
[SwitchA-classifier-vlan203] quit
```

Create a behavior named **car_vlan201_downlink** for rate limiting the upstream traffic of VLAN 201 from Branch C. In the behavior, set the CIR to 400000 kbps and CBS to 2500000 bytes (the number of bytes transmitted over 50 ms at the rate of CIR).

```
[SwitchA] traffic behavior car_vlan201_downlink
[SwitchA-behavior-car_vlan201_downlink] car cir 400000 cbs 2500000
[SwitchA-behavior-car_vlan201_downlink] quit
```

Create behaviors named **car_vlan202_downlink** and **car_vlan203_downlink**, and configure a traffic policing action in each behavior: set the CIR to 200000 kbps and CBS to 1250000 bytes.

```
[SwitchA] traffic behavior car_vlan202_downlink
[SwitchA-behavior-car_vlan202_downlink] car cir 200000 cbs 1250000
[SwitchA-behavior-car_vlan202_downlink] quit
[SwitchA] traffic behavior car_vlan203_downlink
[SwitchA-behavior-car_vlan203_downlink] car cir 200000 cbs 1250000
[SwitchA-behavior-car_vlan203_downlink] quit
```

Create a QoS policy named **downlink_in_c**, and associate the three classes with their specific behaviors in the QoS policy.

```
[SwitchA] qos policy downlink_in_c
[SwitchA-qospolicy-downlink_in_c] classifier vlan201 behavior car_vlan201_downlink
[SwitchA-qospolicy-downlink_in_c] classifier vlan202 behavior car_vlan202_downlink
[SwitchA-qospolicy-downlink_in_c] classifier vlan203 behavior car_vlan203_downlink
[SwitchA-qospolicy-downlink_in_c] quit
```

Apply the QoS policy **downlink_in_c** to the incoming traffic of GigabitEthernet 1/0/3 to rate limit the upstream traffic of VLAN 201, VLAN 202, and VLAN 203 from Branch C.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] qos apply policy downlink_in_c inbound
```

Apply the QoS policy **downlink_in_c** to the outgoing traffic of GigabitEthernet 1/0/3 to rate limit the downstream traffic of VLAN 201, VLAN 202, and VLAN 203 to Branch C.

```
[SwitchA-GigabitEthernet1/0/3] qos apply policy downlink_in_c outbound
```

Perform the following configurations:

- Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/10 as trunk ports.
- Assign them to VLANs 201 through 203.
- Remove them from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 201 to 203
[SwitchA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface GigabitEthernet 1/0/10
[SwitchA-GigabitEthernet1/0/10] port link-type trunk
[SwitchA-GigabitEthernet1/0/10] port trunk permit vlan 201 to 203
[SwitchA-GigabitEthernet1/0/10] undo port trunk permit vlan 1
```

Configuring bandwidth allocation related to VLAN mapping

1. Perform the following configurations:
   - Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports.
   - Assign them to VLANs 1001 through 1003 and VLANs 201 through 203.
   - Remove them from VLAN 1.
   - Enable QinQ on the two interfaces to implement VLAN mapping.

   ```
   [SwitchA] interface GigabitEthernet1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-type trunk
   [SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1001 to 1003 201 to 203
   [SwitchA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   [SwitchA-GigabitEthernet1/0/1] qinq enable
   [SwitchA-GigabitEthernet1/0/1] quit
   [SwitchA] interface GigabitEthernet1/0/2
   [SwitchA-GigabitEthernet1/0/2] port link-type trunk
   [SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1001 to 1003 201 to 203
   [SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
   [SwitchA-GigabitEthernet1/0/2] qinq enable
   [SwitchA-GigabitEthernet1/0/2] quit
   ```

2. Configure classes and behaviors for performing VLAN mapping for the upstream traffic.

   # Create a class named **1001_to_201**, and configure CVLAN 1001 as the match criteria. This class is used in the QoS policy that maps VLAN 1001 to VLAN 201.

   ```
   [SwitchA] traffic classifier 1001_to_201
   [SwitchA-classifier-1001_to_201] if-match customer-vlan-id 1001
   [SwitchA-classifier-1001_to_201] quit
   ```

   # Create a behavior named **1001_to_201**, and configure the action of marking traffic with SVLAN 201 in the behavior.

   ```
   [SwitchA] traffic behavior 1001_to_201
   [SwitchA-behavior-1001_to_201] remark service-vlan-id 201
   [SwitchA-behavior-1001_to_201] quit
   ```

Create classes **1002_to_202** and **1003_to_203** and behaviors **1002_to_202** and **1003_to_203**. They are used for mapping VLAN 1002 to VLAN 202 and VLAN 1003 to VLAN 203.

```
[SwitchA] traffic classifier 1002_to_202
[SwitchA-classifier-1002_to_202] if-match customer-vlan-id 1002
[SwitchA-classifier-1002_to_202] quit
[SwitchA] traffic behavior 1002_to_202
[SwitchA-behavior-1002_to_202] remark service-vlan-id 202
[SwitchA-behavior-1002_to_202] quit
[SwitchA] traffic classifier 1003_to_203
[SwitchA-classifier-1003_to_203] if-match customer-vlan-id 1003
[SwitchA-classifier-1003_to_203] quit
[SwitchA] traffic behavior 1003_to_203
[SwitchA-behavior-1003_to_203] remark service-vlan-id 203
[SwitchA-behavior-1003_to_203] quit
```

3. Configure classes and behaviors for performing VLAN mapping for the downstream traffic.

   # Create a class named **201_to_1001**, and configure SVLAN 1001 as the match criteria. This class is used in the QoS policy that maps VLAN 201 to VLAN 1001.

   ```
   [SwitchA] traffic classifier 201_to_1001
   [SwitchA-classifier-201_to_1001] if-match service-vlan-id 201
   [SwitchA-classifier-201_to_1001] quit
   ```

   # Create a behavior named **201_to_1001**, and configure the action of marking traffic with CVLAN 1001 in the behavior.

   ```
   [SwitchA] traffic behavior 201_to_1001
   [SwitchA-behavior-201_to_1001] remark customer-vlan-id 1001
   [SwitchA-behavior-201_to_1001] quit
   ```

   # Create classes **202_to_1002** and **203_to_1003** and behaviors **202_to_1002** and **203_to_1003**. They are used for mapping VLAN 202 to VLAN 1002 and VLAN 203 to VLAN 1003.

   ```
   [SwitchA] traffic classifier 202_to_1002
   [SwitchA-classifier-202_to_1002] if-match service-vlan-id 202
   [SwitchA-classifier-202_to_1002] quit
   [SwitchA] traffic behavior 202_to_1002
   [SwitchA-behavior-202_to_1002] remark customer-vlan-id 1002
   [SwitchA-behavior-202_to_1002] quit
   [SwitchA] traffic classifier 203_to_1003
   [SwitchA-classifier-203_to_1003] if-match service-vlan-id 203
   [SwitchA-classifier-203_to_1003] quit
   [SwitchA] traffic behavior 203_to_1003
   [SwitchA-behavior-203_to_1003] remark customer-vlan-id 1003
   [SwitchA-behavior-203_to_1003] quit
   ```

4. Configure classes and behaviors to rate limit the upstream traffic from branches.

   According to the requirements analysis, the match criteria for rate limiting the upstream traffic from branches are newly marked VLANs. Therefore, you can use the traffic classes for VLAN 201, VLAN 202, and VLAN 203, which are **201_to_1001**, **202_to_1002**, and **203_to_1003** in this example. The behaviors for policing the traffic can be **car_vlan201_downlink**, **car_vlan202_downlink**, and **car_vlan203_downlink**, which are configured in "Configuring bandwidth allocation unrelated to VLAN mapping."

5. Configure classes and behaviors for rate limiting the downstream traffic sent to branches.

Create a class named **vlan201_downlink**, and configure SVLAN 1001 as the match criteria.

```
[SwitchA] traffic classifier vlan201_downlink
[SwitchA-classifier-vlan201_downlink] if-match service-vlan-id 1001
[SwitchA-classifier-vlan201_downlink] quit
```

NOTE:

When you configure a class for rate limiting the downstream traffic, you must use the **service-vlan-id** criterion. The VLAN specified for the criterion, however, should be the marked customer-side VLAN ID, for example, VLAN 1001.

Create classes **vlan202_downlink** and **vlan203_downlink** in the same way.

```
[SwitchA] traffic classifier vlan202_downlink
[SwitchA-classifier-vlan202_downlink] if-match service-vlan-id 1002
[SwitchA-classifier-vlan202_downlink] quit
[SwitchA] traffic classifier vlan203_downlink
[SwitchA-classifier-vlan203_downlink] if-match service-vlan-id 1003
[SwitchA-classifier-vlan203_downlink] quit
```

Because the rate limit requirements for the downstream traffic are the same as those for the upstream traffic, you can use the behaviors **car_vlan201_downlink**, **car_vlan202_downlink**, and **car_vlan203_downlink**.

6. Configure classes and behaviors for rate-limiting the upstream traffic to the backbone network.

   The match criteria for rate-limiting the upstream traffic are newly marked VLANs (VLAN 201, VLAN 202, and VLAN 203). Therefore, you can use classes **201_to_1001**, **202_to_1002**, and **203_to_1003**.

   # Create a behavior named **car_vlan201_uplink** for rate limiting the upstream traffic of VLAN 201 on Switch A. In the behavior, set the CIR to 100000 kbps and CBS to 625000 bytes (the number of bytes transmitted over 50 ms at the rate of CIR).

   ```
   [SwitchA] traffic behavior car_vlan201_uplink
   [SwitchA-behavior-car_vlan201_uplink] car cir 100000 cbs 625000
   [SwitchA-behavior-car_vlan201_uplink] quit
   ```

   # Create behaviors named **car_vlan202_uplink** and **car_vlan203_uplink** for rate limiting upstream traffic of VLAN 202 and VLAN 203. In the behavior **car_vlan202_uplink**, set the CIR to 60000 kbps and CBS to 375000 bytes. In the behavior **car_vlan203_uplink**, set the CIR to 40000 kbps and CBS to 250000 bytes.

   ```
   [SwitchA] traffic behavior car_vlan202_uplink
   [SwitchA-behavior-car_vlan202_uplink] car cir 60000 cbs 375000
   [SwitchA-behavior-car_vlan202_uplink] quit
   [SwitchA] traffic behavior car_vlan203_uplink
   [SwitchA-behavior-car_vlan203_uplink] car cir 40000 cbs 250000
   [SwitchA-behavior-car_vlan203_uplink] quit
   ```

7. Configure classes and behaviors to rate limit the downstream traffic from the backbone network.

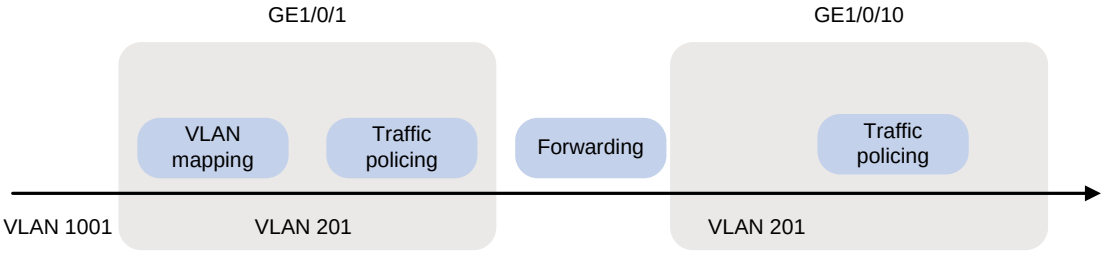
   The match criteria for rate limiting the downstream traffic from the backbone network are newly marked VLANs (VLAN 201, VLAN 202, and VLAN 203). Therefore, you can use classes **201_to_1001**, **202_to_1002**, and **203_to_1003**.

   Because the rate limit requirements for the downstream traffic are the same as those for the upstream traffic, you can use the behaviors **car_vlan201_uplink**, **car_vlan202_uplink**, and **car_vlan203_uplink**.

8. Configure and apply the QoS policies for upstream traffic.

   Figure 181 shows how the switches process the upstream traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.

Figure 181 Upstream traffic processing



   # Create a QoS policy named **downlink_in**, and configure the following class-behavior associations in this order:

   - The VLAN mapping class-behavior associations.
   - The traffic policing class-behavior associations that use the newly marked VLANs as the match criteria.

```
[SwitchA] qos policy downlink_in
[SwitchA-qospolicy-downlink_in] classifier 1001_to_201 behavior 1001_to_201
[SwitchA-qospolicy-downlink_in] classifier 1002_to_202 behavior 1002_to_202
[SwitchA-qospolicy-downlink_in] classifier 1003_to_203 behavior 1003_to_203
[SwitchA-qospolicy-downlink_in] classifier 201_to_1001 behavior
car_vlan201_downlink
[SwitchA-qospolicy-downlink_in] classifier 202_to_1002 behavior
car_vlan202_downlink
[SwitchA-qospolicy-downlink_in] classifier 203_to_1003 behavior
car_vlan203_downlink
[SwitchA-qospolicy-downlink_in] quit
```

   # Apply the QoS policy **downlink_in** to the incoming traffic of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy downlink_in inbound
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy downlink_in inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

   # Create a QoS policy named **uplink_out**, and associate the classes and behaviors configured to rate-limit the upstream traffic to the backbone network.

```
[SwitchA] qos policy uplink_out
[SwitchA-qospolicy-uplink_out] classifier 201_to_1001 behavior car_vlan201_uplink
[SwitchA-qospolicy-uplink_out] classifier 202_to_1002 behavior car_vlan202_uplink
[SwitchA-qospolicy-uplink_out] classifier 203_to_1003 behavior car_vlan203_uplink
[SwitchA-qospolicy-downlink_in] quit
```

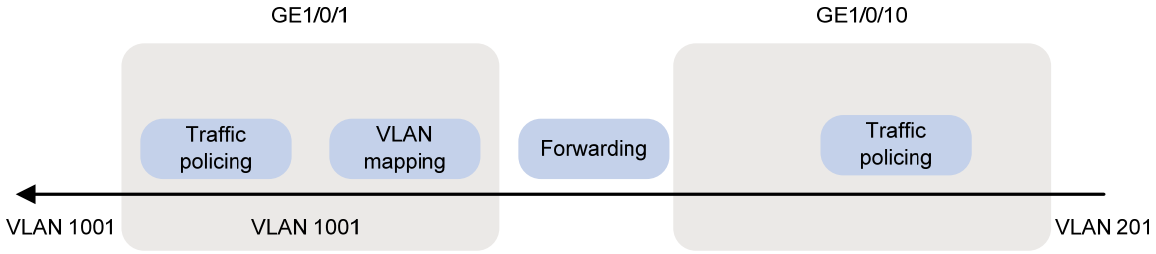
   # Apply QoS policy **uplink_out** to the outgoing traffic of GigabitEthernet 1/0/10.

```
[SwitchA] interface GigabitEthernet1/0/10
[SwitchA-GigabitEthernet1/0/10] qos apply policy uplink_out outbound
```

9. Configure and apply the QoS policies for downstream traffic.

Figure 182 shows how the switches process the downstream traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.

Figure 182 Downstream traffic processing



Create a QoS policy named **uplink_in**, and associate the classes and behaviors configured to rate limit the downstream traffic from the backbone network.

```
[SwitchA] qos policy uplink_in
[SwitchA-qospolicy-uplink_in] classifier 201_to_1001 behavior car_vlan201_uplink
[SwitchA-qospolicy-uplink_in] classifier 202_to_1002 behavior car_vlan202_uplink
[SwitchA-qospolicy-uplink_in] classifier 203_to_1003 behavior car_vlan203_uplink
[SwitchA-qospolicy-uplink_in] quit
```

Apply the QoS policy **uplink_in** to the incoming traffic of GigabitEthernet 1/0/10.

```
[SwitchA] interface GigabitEthernet1/0/10
[SwitchA-GigabitEthernet1/0/10] qos apply policy uplink_in inbound
```

Create a QoS policy named **downlink_out**, and configure the following class-behavior associations in this order:

- The VLAN mapping class-behavior associations.
- The traffic policing class-behavior associations that rate limit the downstream traffic to branches.

```
[SwitchA] qos policy downlink_out
[SwitchA-qospolicy-downlink_out] classifier 201_to_1001 behavior 201_to_1001
[SwitchA-qospolicy-downlink_out] classifier 202_to_1002 behavior 202_to_1002
[SwitchA-qospolicy-downlink_out] classifier 203_to_1003 behavior 203_to_1003
[SwitchA-qospolicy-downlink_out] classifier vlan201_downlink behavior
car_vlan201_downlink
[SwitchA-qospolicy-downlink_out] classifier vlan202_downlink behavior
car_vlan202_downlink
[SwitchA-qospolicy-downlink_out] classifier vlan203_downlink behavior
car_vlan203_downlink
[SwitchA-qospolicy-downlink_in] quit
```

Apply the QoS policy **downlink_out** to the outgoing traffic of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy downlink_out outbound
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy downlink_out outbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuration files

```
#
traffic classifier vlan203_downlink operator and
 if-match service-vlan-id 1003
traffic classifier 1002_to_202 operator and
 if-match customer-vlan-id 1002
traffic classifier 201_to_1001 operator and
 if-match service-vlan-id 201
traffic classifier 1003_to_203 operator and
 if-match customer-vlan-id 1003
traffic classifier 203_to_1003 operator and
 if-match service-vlan-id 203
traffic classifier vlan201 operator and
 if-match service-vlan-id 201
traffic classifier vlan201_downlink operator and
 if-match service-vlan-id 1001
traffic classifier vlan202 operator and
 if-match service-vlan-id 202
traffic classifier vlan202_downlink operator and
 if-match service-vlan-id 1002
traffic classifier 202_to_1002 operator and
 if-match service-vlan-id 202
traffic classifier 1001_to_201 operator and
 if-match customer-vlan-id 1001
traffic classifier vlan203 operator and
 if-match service-vlan-id 203
#
traffic behavior car_vlan201_downlink
 car cir 400000 cbs 2500000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan202_downlink
 car cir 200000 cbs 1250000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan203_downlink
 car cir 200000 cbs 1250000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan201_uplink
 car cir 100000 cbs 625000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan202_uplink
 car cir 60000 cbs 375000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan203_uplink
 car cir 40000 cbs 250000 ebs 512 green pass red discard yellow pass
traffic behavior 1002_to_202
 remark service-vlan-id 202
traffic behavior 201_to_1001
 remark customer-vlan-id 1001
traffic behavior 1003_to_203
 remark service-vlan-id 203
traffic behavior 203_to_1003
 remark customer-vlan-id 1003
```

```
traffic behavior 202_to_1002
 remark customer-vlan-id 1002
traffic behavior 1001_to_201
 remark service-vlan-id 201
#
qos policy uplink_in
 classifier 201_to_1001 behavior car_vlan201_uplink
 classifier 202_to_1002 behavior car_vlan202_uplink
 classifier 203_to_1003 behavior car_vlan203_uplink
qos policy uplink_out
 classifier 201_to_1001 behavior car_vlan201_uplink
 classifier 202_to_1002 behavior car_vlan202_uplink
 classifier 203_to_1003 behavior car_vlan203_uplink
qos policy downlink_in
 classifier 1001_to_201 behavior 1001_to_201
 classifier 1002_to_202 behavior 1002_to_202
 classifier 1003_to_203 behavior 1003_to_203
 classifier 201_to_1001 behavior car_vlan201_downlink
 classifier 202_to_1002 behavior car_vlan202_downlink
 classifier 203_to_1003 behavior car_vlan203_downlink
qos policy downlink_in_c
 classifier vlan201 behavior car_vlan201_downlink
 classifier vlan202 behavior car_vlan202_downlink
 classifier vlan203 behavior car_vlan203_downlink
qos policy downlink_out
 classifier 201_to_1001 behavior 201_to_1001
 classifier 202_to_1002 behavior 202_to_1002
 classifier 203_to_1003 behavior 203_to_1003
 classifier vlan201_downlink behavior car_vlan201_downlink
 classifier vlan202_downlink behavior car_vlan202_downlink
 classifier vlan203_downlink behavior car_vlan203_downlink
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203 1001 to 1003
 qinq enable
 qos apply policy downlink_in inbound
 qos apply policy downlink_out outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203 1001 to 1003
 qinq enable
 qos apply policy downlink_in inbound
```

```
 qos apply policy downlink_out outbound
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203
 qos apply policy uplink_in inbound
 qos apply policy uplink_out outbound
```

Example: Configuring aggregate CAR

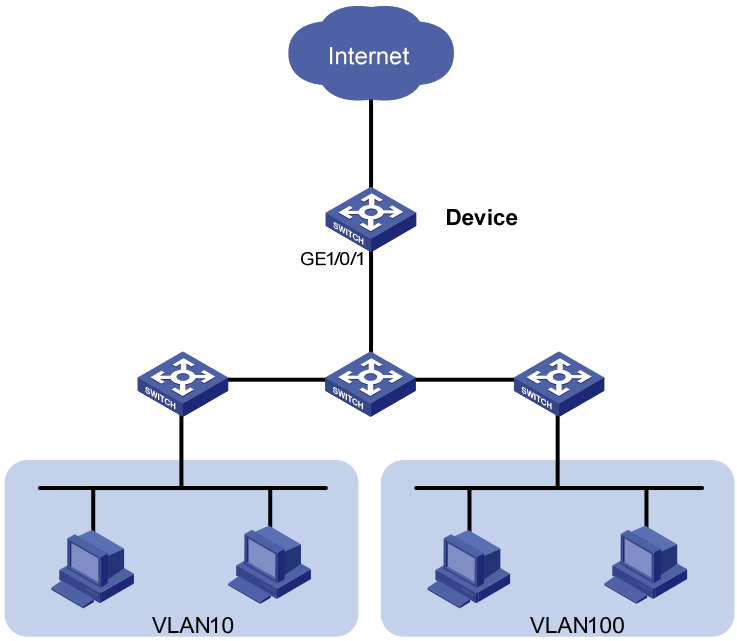
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 183, configure aggregate CAR to limit the incoming traffic from VLAN 10 and VLAN 100 on GigabitEthernet 1/0/1 to 200 Mbps and to drop the excess traffic.

Figure 183 Network diagram



Configuration restrictions and guidelines

In a traffic behavior, the traffic policing action cannot be configured together with a priority marking action (local precedence, drop precedence, 802.1p priority, DSCP, or IP precedence marking). Otherwise, a QoS policy that references such a behavior cannot be applied correctly.

Configuration procedures

In this example, suppose the access layer devices have added VLAN tags for the traffic of VLAN 10 and VLAN 100 and sent the traffic to Device.

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type trunk
```

Assign it to VLANs 10 through 100.

```
[Device-GigabitEthernet1/0/1] port trunk permit vlan 10 100
```

Remove it from VLAN 1.

```
[Device-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/1] quit
```

Create an aggregate CAR action.

```
[Device] qos car aggcar-1 aggregative cir 200000 red discard
```

Configure a class with SVLAN ID 10 as the match criterion, and configure a behavior with the aggregate CAR action.

```
[Device] traffic classifier 1
[Device-classifier-1] if-match service-vlan-id 10
[Device-classifier-1] quit
[Device] traffic behavior 1
[Device-behavior-1] car name aggcar-1
[Device-behavior-1] quit
```

Configure a class with SVLAN ID 100 as the match criterion, and configure a behavior with the aggregate CAR action.

```
[Device] traffic classifier 2
[Device-classifier-2] if-match service-vlan-id 100
[Device-classifier-2] quit
[Device] traffic behavior 2
[Device-behavior-2] car name aggcar-1
[Device-behavior-2] quit
```

Create a QoS policy named **car**, and associate the classes with the behaviors in the QoS policy.

```
[Device] qos policy car
[Device-qospolicy-car] classifier 1 behavior 1
[Device-qospolicy-car] classifier 2 behavior 2
[Device-qospolicy-car] quit
```

Apply the QoS policy **car** to the incoming traffic of GigabitEthernet 1/0/1.

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy car inbound
```

Configuration files

```
#
 qos car aggcar-1 aggregative cir 20000 cbs 1250000 ebs 512 green pass yellow pa
ss red discard
#
traffic classifier 1 operator and
 if-match service-vlan-id 10
traffic classifier 2 operator and
 if-match service-vlan-id 100
#
traffic behavior 1
 car name aggcar-1
traffic behavior 2
 car name aggcar-1
#
qos policy car
 classifier 1 behavior 1
 classifier 2 behavior 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 100
 qos apply policy car inbound
```

GTS and rate limiting configuration examples

This chapter provides GTS and rate limiting configuration examples.

Example: Configuring GTS and rate limiting

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 184, a company connects its branches (on the left) and its headquarters (on the right) through a dedicated line. The dedicated line mainly transmits the FTP traffic, service application traffic, and IP voice traffic.

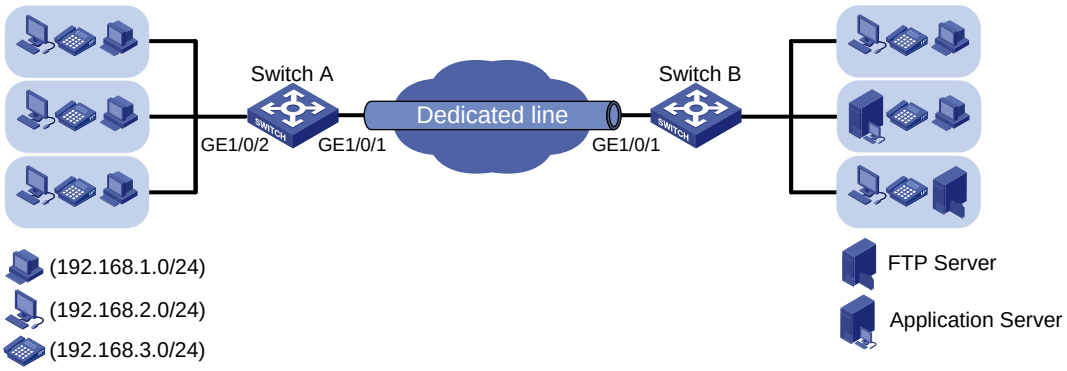
Due to limited dedicated line bandwidth, configure traffic policing on the edge device Switch B of the headquarters, as follows:

- Set the CIR to 10 Mbps for IP voice traffic.
- Set the CIR to 3 Mbps for service application traffic.
- Set the CIR to 7 Mbps for FTP traffic.

To cooperate with the traffic policing configured in the headquarters, configure traffic shaping on edge device Switch A of the branch to buffer the excess bursty traffic and to avoid packet loss.

Additionally, because the dedicated line bandwidth is 20 Mbps, configure rate limiting on Switch A to make sure the total rate of traffic from Switch A to the dedicated line cannot exceed 20 Mbps.

Figure 184 Network diagram



Requirements analysis

To implement GTS, first determine the ID of the queue that transmits a type of traffic. In this example, the priorities of these types of traffic are not provided. You need to use priority marking to manually assign packets to different queues.

You can manually assign packets to queues through marking DSCP values, 802.1p priority values, or local precedence values. In order to keep the packets unchanged, mark local precedence values for packets.

Configuration procedures

IMPORTANT:

Before you configure GTS and rate limiting, make sure the network in Figure 184 is reachable. Information about implementing connectivity on Switch A and Switch B (for example, creating VLAN-interfaces and assigning IP addresses to VLAN-interfaces) is not shown.

Configuring priority marking

1. Create three classes on Switch A to match the three types of traffic by source IP address:

   # Configure IPv4 basic ACL 2000 to match the traffic from IP phones on network segment 192.168.3.0/24.

```
<SwitchA> system-view
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 192.168.3.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

   # Create a class named **voice**, and use IPv4 ACL 2000 as the match criterion in the class.

```
[SwitchA] traffic classifier voice
[SwitchA-classifier-voice] if-match acl 2000
[SwitchA-classifier-voice] quit
```

   # Configure IPv4 basic ACL 2001 to match the traffic from the service software endpoints on network segment 192.168.2.0/24.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[SwitchA-acl-basic-2001] quit
```

   # Create a class named **service**, and use IPv4 ACL 2001 as the match criterion in the class.

```
[SwitchA] traffic classifier service
[SwitchA-classifier-service] if-match acl 2001
[SwitchA-classifier-service] quit
```

   # Configure IPv4 advanced ACL 3000 to match the FTP traffic with the destination port 20 from common PCs (on network segment 192.168.1.0/24).

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 20 source 192.168.1.0
0.0.0.255
[SwitchA-acl-adv-3000] quit
```

   # Create a class named **ftp**, and use IPv4 ACL 3000 as the match criterion in the class.

```
[SwitchA] traffic classifier ftp
```

```
[SwitchA-classifier-ftp] if-match acl 3000
[SwitchA-classifier-ftp] quit
```

2. Create three traffic behaviors, and configure the actions of setting the local precedence values to 6, 4, and 2, respectively:

   # Create a behavior named **voice**, and configure the action of setting the local precedence value to 6 for the behavior.

```
[SwitchA] traffic behavior voice
[SwitchA-behavior-voice] remark local-precedence 6
[SwitchA-behavior-voice] quit
```

   # Create a behavior named **service**, and configure the action of setting the local precedence value to 4 for the behavior.

```
[SwitchA] traffic behavior service
[SwitchA-behavior-service] remark local-precedence 4
[SwitchA-behavior-service] quit
```

   # Create a behavior named **ftp**, and configure the action of setting the local precedence value to 2 for the behavior.

```
[SwitchA] traffic behavior ftp
[SwitchA-behavior-ftp] remark local-precedence 2
[SwitchA-behavior-ftp] quit
```

3. Configure a QoS policy and apply the QoS policy:

   # Create a QoS policy named **shaping**, and associate classes with the corresponding traffic behaviors in the QoS policy.

```
[SwitchA] qos policy shaping
[SwitchA-qospolicy-shaping] classifier voice behavior voice
[SwitchA-qospolicy-shaping] classifier service behavior service
[SwitchA-qospolicy-shaping] classifier ftp behavior ftp
[SwitchA-qospolicy-shaping] quit
```

   # Apply the QoS policy to the incoming traffic of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy shaping inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

After the configuration above, the local precedence values of the three traffic flows are changed, and you can determine that IP voice traffic, service application traffic, and FTP traffic are assigned to queues 6, 4, and 2, respectively.

Configuring GTS

Configure traffic shaping on port GigabitEthernet 1/0/1, and set the CIR to 10000 kbps for queue 6.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos gts queue 6 cir 10000
```

Configure traffic shaping on port GigabitEthernet 1/0/1, and set the CIR to 3000 kbps for queue 4.

```
[SwitchA-GigabitEthernet1/0/1] qos gts queue 4 cir 3000
```

Configure traffic shaping on port GigabitEthernet 1/0/1, and set the CIR to 7000 kbps for queue 2.

```
[SwitchA-GigabitEthernet1/0/1] qos gts queue 2 cir 7000
```

Configuring rate limiting

Configure rate limiting on port GigabitEthernet 1/0/1, and set the CIR to 20000 kbps for the outgoing traffic of the port.

```
[SwitchA-GigabitEthernet1/0/1] qos lr outbound cir 20000
```

Verifying the configuration

Use the **display qos gts interface** command to display traffic shaping configuration.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
 Rule(s): If-match queue 6
 CIR 10000 (kbps), CBS 625152 (byte)
 Rule(s): If-match queue 4
 CIR 7000 (kbps), CBS 437760 (byte)
 Rule(s): If-match queue 2
 CIR 3000 (kbps), CBS 187904 (byte)
```

Use the **display qos lr interface** command to display the rate limiting configuration of a port.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
 CIR 20000 (kbps),  CBS 1250304 (byte)
```

Configuration files

```
#
acl number 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
acl number 2001
 rule 0 permit source 192.168.2.0 0.0.0.255
#
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp-data
#
traffic classifier service operator and
 if-match acl 2001
traffic classifier ftp operator and
 if-match acl 3000
traffic classifier voice operator and
 if-match acl 2000
#
traffic behavior service
 remark local-precedence 4
traffic behavior ftp
 remark local-precedence 2
traffic behavior voice
 remark local-precedence 6
#
qos policy shaping
 classifier voice behavior voice
 classifier service behavior service
```

```
 classifier ftp behavior ftp
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos lr outbound cir 20000 cbs 1250304
 qos gts queue 6 cir 10000 cbs 625152
 qos gts queue 4 cir 7000 cbs 437760
 qos gts queue 2 cir 3000 cbs 187904
#
interface GigabitEthernet1/2/0/2
 port link-mode bridge
 qos apply policy shaping inbound
```

Priority and queue scheduling configuration examples

This chapter provides priority mapping, priority marking, and queue scheduling configuration examples.

When the network is congested, these functions can preferentially send critical data traffic and provide efficient, differentiated transmission services.

Example: Configuring priority mapping and queue scheduling

Applicable product matrix

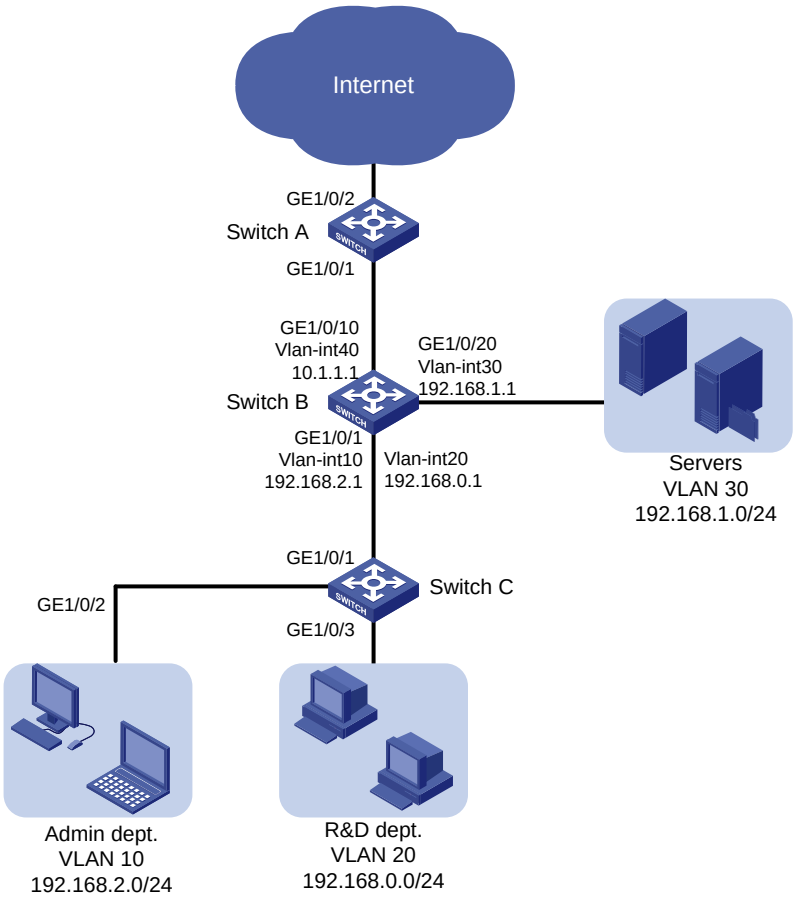
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

The network diagram of a company is as shown in Figure 185. Configure priority mapping and queue scheduling to tune the internal network traffic and Internet-accessing traffic on each device to satisfy the following requirements:

- **Access to the internal server farm**—The traffic from the Administration department takes priority over that from the R&D department. When the network is congested, they are scheduled in the ratio of 2:1.
- **Access to the Internet**—The traffic from the Administration department takes priority over that from the R&D department. When the network is congested, the traffic from the Administration department is scheduled preferentially, and the traffic from the R&D department is scheduled when no traffic from the Administration department exists.
- The Internet-accessing traffic includes the following types: HTTP, FTP, and Email, with the DSCP values 33, 35, and 27, respectively. Transmit the three types of traffic in the following priority order: HTTP > FTP > Email. When congestion occurs, the three types of traffic are transmitted in the ratio of 2:1:1.

Figure 185 Network diagram



Requirements analysis

Priority configuration for the internal network traffic

To prioritize packets by department, configure different port priorities for the ports connected to the two departments, so that the packets from the two departments are marked with different 802.1p priorities.

To make the marked 802.1p priority actually affect the packet transmission, configure trusting the 802.1p priorities of received packets on all incoming ports along the transmission path, so that the devices can enqueue packets by 802.1p priority.

To satisfy the packet scheduling ratio when congestion occurs, configure WRR on port GigabitEthernet 1/0/20 of Switch B and configure different weights for queues.

Priority configuration for the Internet traffic

To absolutely prioritize the traffic from the Administration department when the port is congested in the outbound direction, perform the following configurations:

- Configure SP queuing on the port.
- Assign the traffic from the Administration department to a higher-priority queue.

The 802.1p priority mapping cannot satisfy the requirements of determining the transmission priority based on the upper-layer protocols. To satisfy the requirement, configure trusting the DSCP values on the port, so that the port can enqueue packets based on the DSCP values.

To schedule packets from different queues in a specified ratio when congestion occurs, use WRR queuing and configure different weights for queues.

Configuration procedures

Configuring transmission priorities for the internal network traffic

1. Configure Switch C:

   # Create VLANs 10 and 20.

   ```
   <SwitchC> system-view
   [SwitchC] vlan 10
   [SwitchC-vlan10] quit
   [SwitchC] vlan 20
   [SwitchC-vlan20] quit
   ```

   # Assign port GigabitEthernet 1/0/2 to VLAN 10. Set the port priority to 6 for the port, so that the traffic from the Administration department is marked with 802.1p priority value 6.

   ```
   [SwitchC] interface GigabitEthernet 1/0/2
   [SwitchC-GigabitEthernet1/0/2] port access vlan 10
   [SwitchC-GigabitEthernet1/0/2] qos priority 6
   [SwitchC-GigabitEthernet1/0/2] quit
   ```

   # Assign port GigabitEthernet 1/0/3 to VLAN 20. Set the port priority to 4 for the port, so that the traffic from the R&D department is marked with 802.1p priority value 4.

   ```
   [SwitchC] interface GigabitEthernet 1/0/3
   [SwitchC-GigabitEthernet1/0/3] port access vlan 20
   [SwitchC-GigabitEthernet1/0/3] qos priority 4
   [SwitchC-GigabitEthernet1/0/3] quit
   ```

   # Because the 802.1p priorities are carried in VLAN tags, you must configure GigabitEthernet 1/0/1 to send packets carrying VLAN tags. This example uses the port link type **trunk**. Assign the port to VLAN 10 and VLAN 20. The port is in VLAN 1 by default, so you must remove the port from VLAN 1.

   ```
   [SwitchC] interface GigabitEthernet 1/0/1
   [SwitchC-GigabitEthernet1/0/1] port link-type trunk
   [SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 10 20
   [SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   [SwitchC-GigabitEthernet1/0/1] quit
   ```

2. Configure Switch B:

   # Create VLANs 10, 20, 30, and 40.

   ```
   <SwitchB> system-view
   [SwitchB] vlan 10
   [SwitchB-vlan10] quit
   [SwitchB] vlan 20
   [SwitchB-vlan20] quit
   [SwitchB] vlan 30
   [SwitchB-vlan30] quit
   [SwitchB] vlan 40
   [SwitchB-vlan40] quit
   ```

   # Configure GigabitEthernet 1/0/1 as a trunk port.

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 10 and 20.

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

Remove the port from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure port GigabitEthernet 1/0/1 to trust the 802.1p priorities of received packets. By default, a port trusts 802.1p priorities of received packets. Skip this step if the default priority trust mode is used.

```
[SwitchB-GigabitEthernet1/0/1] undo qos trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign port GigabitEthernet 1/0/10 to VLAN 40.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port access vlan 40
```

Assign port GigabitEthernet 1/0/20 to VLAN 30.

```
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] port access vlan 30
```

NOTE:

On Switch B, you must create VLAN-interfaces and configure routing protocols to enable communication between network segments. For more information about these configurations, see the routing configuration examples.

Based on the 802.1p-to-local priority mapping table, traffic with 802.1p priority 4 is assigned to queue 4, and traffic with 802.1p priority 6 is assigned to queue 6.

Configure WRR on egress port GigabitEthernet 1/0/20, and configure the weight of queue 6 as two times as great as that of queue 4. In this example, set the weight value to 4 for queue 6 and 2 for queue 4.

```
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] qos wrr
[SwitchB-GigabitEthernet1/0/20] qos wrr 4 group 1 weight 2
[SwitchB-GigabitEthernet1/0/20] qos wrr 6 group 1 weight 4
[SwitchB-GigabitEthernet1/0/20] quit
```

Configuring transmission priorities for the traffic to the Internet

1. Configure Switch B:

   # Enable SP queuing on port GigabitEthernet 1/0/10.

   ```
   [SwitchB] interface GigabitEthernet 1/0/10
   [SwitchB-GigabitEthernet1/0/10] qos sp
   ```

2. Configure Switch A:

   # Configure port GigabitEthernet 1/0/1 to trust the DSCP values of received packets.

   ```
   [SwitchA] interface GigabitEthernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] qos trust dscp
   ```

   # DSCP values are mapped to local precedence values based on the DSCP-to-802.1p priority mapping table and then the 802.1p-to-local priority mapping table. Based on the two priority

mapping tables, DSCP values 33, 35, 27 are mapped to local precedence values 4, 4, and 3. According to the network requirements, packets with DSCP value 33 must be assigned to a higher-priority queue. To satisfy this requirement, modify the DSCP-to-802.1p priority mapping table. For example, to map DSCP value 33 to queue 5, map DSCP value 33 to 802.p priority 5 in the DSCP-to-802.1p priority mapping table.

```
[SwitchA] qos map-table dscp-dot1p
[SwitchA-maptbl-dscp-dot1p] import 33 export 5
[SwitchA-maptbl-dscp-dot1p] quit
```

The configuration above assigns the three types of packets to queues 5, 4, and 3, respectively. Configure WRR queuing on GigabitEthernet 1/0/2, and set the weights of the three queues in the ratio of 2:1:1 (6, 3, and 3, for example).

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos wrr
[SwitchA-GigabitEthernet1/0/2] qos wrr 5 group 1 weight 6
[SwitchA-GigabitEthernet1/0/2] qos wrr 4 group 1 weight 3
[SwitchA-GigabitEthernet1/0/2] qos wrr 3 group 1 weight 3
```

Configuration files

- Switch A:

```
#
qos map-table dscp-dot1p
 import 33 export 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos trust dscp
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos wrr
 qos wrr 5 group 1 weight 6
 qos wrr 4 group 1 weight 3
 qos wrr 3 group 1 weight 3
```

- Switch B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 40
#
interface GigabitEthernet1/0/20
 port link-mode bridge
 port access vlan 30
 qos wrr
 qos wrr 6 group 1 weight 4
 qos wrr 4 group 1 weight 2
```

- Switch C:

```
#
vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 qos priority 6
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 20
 qos priority 4
```

Example: Configuring priority marking and queue scheduling

Applicable product matrix

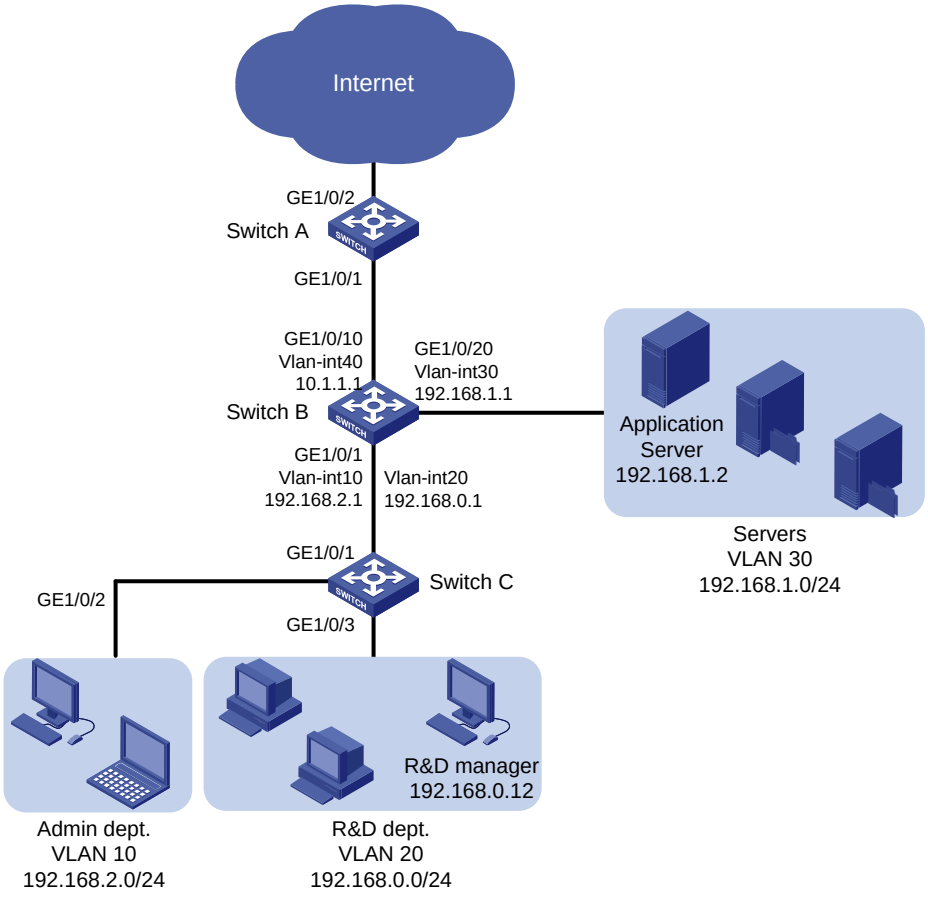
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

The network diagram of a company is as shown in Figure 186. Tune the internal network traffic and Internet-accessing traffic of the company on each device to satisfy the following requirements:

- **Access to the internal server farm**—The traffic from the Administration department takes priority over that from the R&D department. When the network is congested, they are scheduled in the ratio of 2:1. However, the traffic accessing the application server is prioritized regardless of the source department. After the application server traffic transmission, the traffic to the other servers is transmitted in the specified ratio.
- **Access to the Internet**—The traffic from the Administration department takes priority over that from the R&D department. When the network is congested, the traffic from the Administration department is scheduled preferentially. The traffic from the R&D department is scheduled when no traffic from the Administration department exists. However, the Internet-accessing traffic from the R&D department manager is assigned the same priority as the Internet-accessing traffic from the Administration department.
- The Internet-accessing traffic includes the following types: HTTP, FTP, and Email, with the DSCP values 33, 35, and 27, respectively. Transmit the three types of traffic in the following priority order: HTTP>FTP>Email. When congestion occurs, the three types of traffic are transmitted in the ratio of 2:1:1. The email traffic of the Administration department is assigned the same priority as the HTTP traffic.

Figure 186 Network diagram



Requirements analysis

Priority configuration for the internal network traffic

For information about meeting the transmission requirements for traffic that accesses the server farm (except for the application server), see "Requirements analysis." To meet the special requirements of the traffic that accesses the application server, configure priority marking.

Priority marking is configured in a QoS policy. In this example, configure a class to match the traffic destined to the application server IP address. Configure a local precedence value marking traffic behavior for the class of traffic, so that all traffic that accesses the application server can be assigned to an individual queue. Then, configure SP + WRR queuing on port GigabitEthernet 1/0/20 to preferentially transmit the traffic that accesses the application server.

Priority configuration for the Internet traffic

For information about configuring general-purpose priorities for the Internet-accessing traffic, see "Requirements analysis." For the traffic from the R&D department manager, perform the following configurations:

- Configure a class to match the traffic with the specified source IP address.
- Configure a 802.1p priority marking behavior for the class of traffic on Switch C.

As a result, when the traffic from the R&D department manager reaches Switch B, the traffic can be assigned the same local precedence value as the traffic from the Administration department.

For the email traffic from the Administration department, you can perform the following configurations:

- Configure a class to match the traffic with DSCP value 27.
- Configure a priority marking behavior to mark the class of traffic with the same local precedence value as the HTTP traffic.

Configuration procedures

Configuring transmission priorities for the internal network traffic

1. Configure Switch C:

   # Create VLANs 10 and 20.

   ```
   <SwitchC> system-view
   [SwitchC] vlan 10
   [SwitchC-vlan10] quit
   [SwitchC] vlan 20
   [SwitchC-vlan20] quit
   ```

   # Assign port GigabitEthernet 1/0/2 to VLAN 10. Set the port priority to 6 for the port, so that the traffic from the Administration department is marked with 802.1p priority value 6.

   ```
   [SwitchC] interface GigabitEthernet 1/0/2
   [SwitchC-GigabitEthernet1/0/2] port access vlan 10
   [SwitchC-GigabitEthernet1/0/2] qos priority 6
   [SwitchC-GigabitEthernet1/0/2] quit
   ```

   # Assign port GigabitEthernet 1/0/3 to VLAN 20. Set the port priority to 4 for the port, so that the traffic from the R&D department is marked with 802.1p priority value 4.

   ```
   [SwitchC] interface GigabitEthernet 1/0/3
   [SwitchC-GigabitEthernet1/0/3] port access vlan 20
   ```

```
[SwitchC-GigabitEthernet1/0/3] qos priority 4
[SwitchC-GigabitEthernet1/0/3] quit
```

Because the 802.1p priorities are carried in VLAN tags, you must configure GigabitEthernet 1/0/1 to send packets carrying VLAN tags. This example uses the port link type **trunk**. Assign the port to VLAN 10 and VLAN 20. The port is in VLAN 1 by default, so you must remove the port from VLAN 1.

```
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/1] quit
```

2. Configure Switch B:

Create VLANs 10, 20, 30, and 40.

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] vlan 20
[SwitchB-vlan20] quit
[SwitchB] vlan 30
[SwitchB-vlan30] quit
[SwitchB] vlan 40
[SwitchB-vlan40] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 10 and 20.

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

Remove the port from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure port GigabitEthernet 1/0/1 to trust the 802.1p priorities of received packets. By default, a port trusts 802.1p priorities of received packets. Skip this step if the default priority trust mode is used.

```
[SwitchB-GigabitEthernet1/0/1] undo qos trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign port GigabitEthernet 1/0/10 to VLAN 40.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port access vlan 40
```

Assign port GigabitEthernet 1/0/20 to VLAN 30.

```
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] port access vlan 30
```

NOTE:

On Switch B, you must create VLAN-interfaces and configure routing protocols to enable communication between network segments. For more information about these configurations, see the routing configuration examples.

Based on the 802.1p-to-local priority mapping table, traffic with 802.1p priority 4 is assigned to queue 4, and traffic with 802.1p priority 6 is assigned to queue 6.

Configure IPv4 advanced ACL 3000 to match the traffic with the destination IP address 192.168.1.2.

```
[SwitchB] acl number 3000
[SwitchB-acl-adv-3000] rule permit ip destination 192.168.1.2 0
[SwitchB-acl-adv-3000] quit
```

Create a class named **app_server**, and use IPv4 ACL 3000 as the match criterion in the class.

```
[SwitchB] traffic classifier app_server
[SwitchB-classifier-app_server] if-match acl 3000
[SwitchB-classifier-app_server] quit
```

Create a behavior named **app_server**, and configure the action of setting the local precedence value to 7 for the behavior.

```
[SwitchB] traffic behavior app_server
[SwitchB-behavior-app_server] remark local-precedence 7
[SwitchB-behavior-app_server] quit
```

Create a QoS policy named **app_server**, and associate class **app_server** with traffic behavior **app_server** in the QoS policy.

```
[SwitchB] qos policy app_server
[SwitchB-qospolicy-app_server] classifier app_server behavior app_server
[SwitchB-qospolicy-app_server] quit
```

Apply QoS policy **app_server** to the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] qos apply policy app_server inbound
[SwitchB-GigabitEthernet1/0/1] quit
```

Configure SP + WRR queuing on egress port GigabitEthernet 1/0/20.

```
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] qos wrr
```

Configure queue 7 as an SP queue.

```
[SwitchB-GigabitEthernet1/0/20] qos wrr 7 group sp
```

Configure queues 4 and 6 as WRR queues. Configure the weight of queue 6 as two times as great as that of queue 4. In this example, set the weight value to 4 for queue 6 and 2 for queue 4.

```
[SwitchB-GigabitEthernet1/0/20] qos wrr 6 group 1 weight 4
[SwitchB-GigabitEthernet1/0/20] qos wrr 4 group 1 weight 2
```

Configuring transmission priorities for the traffic to the Internet

1. Configure Switch C:

Configure IPv4 basic ACL 2000 to match the traffic with source IP address 192.168.0.12.

```
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 192.168.0.12 0
[SwitchC-acl-basic-2000] quit
```

Create a class named **rd_manager**, and use IPv4 ACL 2000 as the match criterion in the class.

```
[SwitchC] traffic classifier rd_manager
[SwitchC-classifier-rd_manager] if-match acl 2000
[SwitchC-classifier-rd_manager] quit
```

Create a behavior named **rd_manager**, and configure the action of setting the 802.1p priority value to 6 for the behavior.

```
[SwitchC] traffic behavior rd_manager
[SwitchC-behavior-rd_manager] remark dot1p 6
[SwitchC-behavior-rd_manager] quit
```

Create a QoS policy named **rd_manager**, and associate class **rd_manager** with traffic behavior **rd_manager** in the QoS policy.

```
[SwitchC] qos policy rd_manager
[SwitchC-qospolicy-rd_manager] classifier rd_manager behavior rd_manager
[SwitchC-qospolicy-rd_manager] quit
```

Apply QoS policy **rd_manager** to the incoming traffic of GigabitEthernet 1/0/3.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] qos apply policy rd_manager inbound
[SwitchC-GigabitEthernet1/0/3] quit
```

2. Configure Switch B:

Enable SP queuing on port GigabitEthernet 1/0/10.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] qos sp
```

3. Configure Switch A:

Configure port GigabitEthernet 1/0/1 to trust the DSCP values of received packets.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos trust dscp
```

DSCP values are mapped to local precedence values through the DSCP-to-802.1p priority mapping table and then the 802.1p-to-local priority mapping table. Based on the two priority mapping tables, DSCP values 33, 35, 27 are mapped to local precedence values 4, 4, and 3. According to the network requirements, packets with DSCP value 33 must be assigned to a higher-priority queue. To satisfy this requirement, modify the DSCP-to-802.1p priority mapping table. For example, to map DSCP value 33 to queue 5, map DSCP value 33 to 802.p priority 5 in the DSCP-to-802.1p priority mapping table.

```
[SwitchA] qos map-table dscp-dot1p
[SwitchA-maptbl-dscp-dot1p] import 33 export 5
[SwitchA-maptbl-dscp-dot1p] quit
```

The configuration above assigns the three types of packets to queues 5, 4, and 3, respectively. Configure WRR queuing on GigabitEthernet 1/0/2, and set the weights for the three queues in the ratio of 2:1:1 (6, 3, and 3, for example).

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos wrr
[SwitchA-GigabitEthernet1/0/2] qos wrr 5 group 1 weight 6
[SwitchA-GigabitEthernet1/0/2] qos wrr 4 group 1 weight 3
[SwitchA-GigabitEthernet1/0/2] qos wrr 3 group 1 weight 3
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure IPv4 advanced ACL 3000 to match the traffic that is sourced from network segment 192.168.2.0/24 that carries DSCP value 27.

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit ip dscp 27 source 192.168.2.0 0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Create a class named **admin_email**, and use IPv4 ACL 3000 as the match criterion in the class.

```
[SwitchA] traffic classifier admin_email
[SwitchA-classifier-admin_email] if-match acl 3000
[SwitchA-classifier-admin_email] quit
```

Create a behavior named **admin_email**, and configure the action of setting the local precedence value to 5 for the behavior.

```
[SwitchA] traffic behavior admin_email
[SwitchA-behavior-admin_email] remark local-precedence 5
[SwitchA-behavior-admin_email] quit
```

Create a QoS policy named **admin_email**, and associate class **admin_email** with traffic behavior **admin_email** in the QoS policy.

```
[SwitchA] qos policy admin_email
[SwitchA-qospolicy-admin_email] classifier admin_email behavior admin_email
[SwitchA-qospolicy-admin_email] quit
```

Apply QoS policy **admin_email** to the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy admin_email inbound
[SwitchA-GigabitEthernet1/0/1] quit
```

Configuration files

- Switch A:

```
#
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 dscp 27
#
traffic classifier admin_email operator and
 if-match acl 3000
#
traffic behavior admin_email
 remark local-precedence 5
#
qos policy admin_email
 classifier admin_email behavior admin_email
#
qos map-table dscp-dot1p
 import 33 export 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos apply policy admin_email inbound
 qos trust dscp
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos wrr
 qos wrr 5 group 1 weight 6
 qos wrr 4 group 1 weight 3
 qos wrr 3 group 1 weight 3
```

- Switch B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
acl number 3000
 rule 0 permit ip destination 192.168.1.2 0
#
traffic classifier app_server operator and
 if-match acl 3000
#
traffic behavior app_server
 remark local-precedence 7
#
qos policy app_server
 classifier app_server behavior app_server
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 qos apply policy app_server inbound
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 40
#
interface GigabitEthernet1/0/20
 port link-mode bridge
 port access vlan 30
 qos wrr
 qos wrr 7 group sp
 qos wrr 6 group 1 weight 4
 qos wrr 4 group 1 weight 2
```

- Switch C:

```
#
vlan 10
#
vlan 20
#
acl number 2000
 rule 0 permit source 192.168.0.12 0
```

```
#
traffic classifier rd_manager operator and
 if-match acl 2000
#
traffic behavior rd_manager
 remark dot1p 6
#
qos policy rd_manager
 classifier rd_manager behavior rd_manager
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 qos priority 6
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 20
 qos apply policy rd_manager inbound
 qos priority 4
```

User profile configuration examples

This chapter provides configuration examples for applying QoS policies to authenticated users through user profiles.

User profiles contain QoS policies for 802.1X and Portal users. You can configure a user profile and associate the user profile with a user on the authentication server. After the user passes authentication, the authentication server assigns the user profile to the access device. The access device uses the user profile to control the traffic of the user.

Example: Applying QoS policies to authenticated users through user profiles

Applicable product matrix

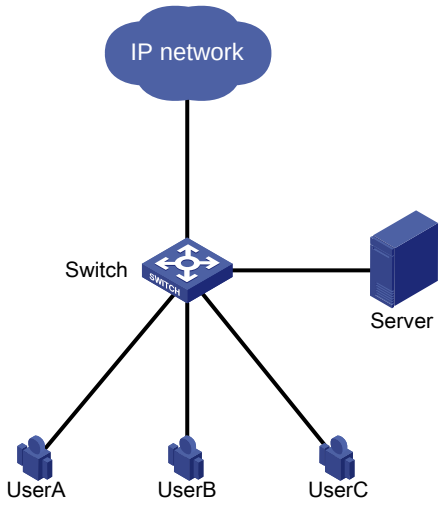
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 187, a switch connects to three 802.1X users through different ports. The users might move to other ports. Configure traffic control to achieve the following purposes:

- Limit the maximum upload rate to 1 M for User A after User A passes authentication.
- Do not allow User B to access the network from 8:30 to 12:00 every day, regardless of whether User B passes authentication.
- Set the 802.1p priority to 5 for the traffic from User C.

Figure 187 Network diagram



Requirements analysis

To allow users to move to other ports, configure user profiles and associate the user profiles to the users.

To limit the upload rate of User A, configure traffic policing.

To not allow User B to access the network from 8:30 to 12:00 every day, use a time range-based ACL and a traffic filtering action.

To mark the 802.1p priority for traffic from User C, use the traffic remark function.

Configuration restrictions and guidelines

When you apply QoS policies to authenticated users through user profiles, follow these restrictions and guidelines:

- If a user profile has been enabled, you can modify the ACL referenced by the QoS policy in the user profile. However, you cannot modify other contents of the QoS policy or delete the QoS policy. If the user associated with the user profile has been online, you also cannot modify the ACL referenced by the QoS policy.
- The traffic behaviors of a QoS policy that applies to a user profile only support the **remark**, **car**, and **filter** actions.
- A QoS policy that applies to a user profile must have contents. Otherwise, the user profile cannot be enabled.

Configuration procedures

Configuring user authentication

Configure 802.1X authentication on the switch and the authentication server. For details, see *802.1X Configuration Examples*.

Configuring QoS policies

1. Configure a QoS policy to limit the upload rate of User A.

Configure a traffic classifier **for_usera** to match all traffic.

After you apply a QoS policy to a user profile, the QoS policy automatically adds match criteria to match the MAC address (**macbased**) or IP address (**portbased**) of users. Therefore, you only need to configure the traffic classifier to match all traffic. The same is true for User B and User C.

```
<Switch> system-view
[Switch] traffic classifier for_usera
[Switch-classifier-for_usera] if-match any
[Switch-classifier-for_usera] quit
```

Configure a traffic behavior **for_usera** to limit the upload rate to 1 M (1024 kbps) for User A.

```
[Switch] traffic behavior for_usera
[Switch-behavior-for_usera] car cir 1024
[Switch-behavior-for_usera] quit
```

Configure a QoS policy **for_usera** that binds the traffic classifier **for_usera** to the traffic behavior **for_usera**.

```
[Switch] qos policy for_usera
[Switch-qospolicy-for_usera] classifier for_usera behavior for_usera
[Switch-qospolicy-for_usera] quit
```

2. Configure a QoS policy to not allow User B to access the network from 8:30 to 12:00 every day.

Configure a time range **for_userb** that defines 8:30 to 12:00 every day.

```
[Switch] time-range for_userb 8:30 to 12:00 daily
```

Configure basic ACL 2000 to match all traffic within the time range **for_userb**.

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit time-range for_userb
[Switch-acl-basic-2000] quit
```

Configure a traffic classifier **for_userb** to match the traffic permitted by ACL 2000.

```
[Switch] traffic classifier for_userb
[Switch-classifier-for_userb] if-match acl 2000
[Switch-classifier-for_userb] quit
```

Configure a traffic behavior **for_userb** to deny the matching traffic.

```
[Switch] traffic behavior for_userb
[Switch-behavior-for_userb] filter deny
[Switch-behavior-for_userb] quit
```

Configure a QoS policy **for_userb** that binds the traffic classifier **for_userb** to the traffic behavior **for_userb**.

```
[Switch] qos policy for_userb
[Switch-qospolicy-for_userb] classifier for_userb behavior for_userb
[Switch-qospolicy-for_userb] quit
```

3. Configure a QoS policy to mark the 802.1p priority for traffic from User C.

Configure a traffic classifier **for_userc** to match all traffic.

```
[Switch] traffic classifier for_userc
[Switch-classifier-for_userc] if-match any
[Switch-classifier-for_userc] quit
```

Configure a traffic behavior **for_userc** to set the 802.1p priority as 5.

```
[Switch] traffic behavior for_userc
[Switch-behavior-for_userc] remark dot1p 5
[Switch-behavior-for_userc] quit
```

Configure a QoS policy **for_userc** that binds the traffic classifier **for_userc** to the traffic behavior **for_userc**.

```
[Switch] qos policy for_userc
[Switch-qospolicy-for_userc] classifier for_userc behavior for_userc
[Switch-qospolicy-for_userc] quit
```

Creating user profiles and applying QoS policies to user profiles

1. Create a user profile for User A.

   # Create a user profile **usera**.

   ```
   [Switch] user-profile usera
   [Switch-user-profile-usera]
   ```

   # Apply the QoS policy **for_usera** to the user profile in the inbound direction to limit the upload rate of User A.

   ```
   [Switch-user-profile-usera] qos apply policy for_usera inbound
   [Switch-user-profile-usera] quit
   ```

   # Enable the user profile.

   ```
   [Switch] user-profile usera enable
   ```

   # Configure the authentication server to assign the user profile **usera** after User A passes authentication. For details, see the user manual of the authentication server.

2. Create a user profile for User B.

   # Create a user profile **userb**.

   ```
   [Switch] user-profile userb
   [Switch-user-profile-userb]
   ```

   # Apply the QoS policy **for_userb** to the user profile in the inbound direction to filter traffic from User B.

   ```
   [Switch-user-profile-userb] qos apply policy for_userb inbound
   [Switch-user-profile-userb] quit
   ```

   # Enable the user profile.

   ```
   [Switch] user-profile userb enable
   ```

   # Configure the authentication server to assign the user profile **userb** after User B passes authentication.

3. Create a user profile for User C.

   # Create a user profile **userc**.

   ```
   [Switch] user-profile userc
   [Switch-user-profile-userc]
   ```

   # Apply the QoS policy **for_userc** to the user profile in the inbound direction to set the 802.1p priority for traffic from User C.

   ```
   [Switch-user-profile-userc] qos apply policy for_userc inbound
   [Switch-user-profile-userc] quit
   ```

   # Enable the user profile.

   ```
   [Switch] user-profile userc enable
   ```

   # Configure the authentication server to assign the user profile **userc** after User C passes authentication.

Verifying the configuration

Display QoS policies.

```
<Switch> display qos policy user-defined

  User Defined QoS Policy Information:

  Policy: for_usera
   Classifier: for_usera
     Behavior: for_usera
      Committed Access Rate:
        CIR 1024 (kbps), CBS 64000 (byte), EBS 512 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass

  Policy: for_userb
   Classifier: for_userb
     Behavior: for_userb
      Filter enable: deny

  Policy: for_userc
   Classifier: for_userc
     Behavior: for_userc
      Marking:
        Remark dot1p COS 5
```

Configuration files

```
#
 time-range for_userb 08:30 to 12:00 daily
#
acl number 2000
 rule 0 permit time-range for_userb
#
traffic classifier for_usera operator and
 if-match any
traffic classifier for_userb operator and
 if-match acl 2000
traffic classifier for_userc operator and
 if-match any
#
traffic behavior for_usera
 car cir 1024 cbs 64000 ebs 512 green pass red discard yellow pass
traffic behavior for_userb
 filter deny
traffic behavior for_userc
 remark dot1p 5
```

```
#
qos policy for_usera
 classifier for_usera behavior for_usera
qos policy for_userb
 classifier for_userb behavior for_userb
qos policy for_userc
 classifier for_userc behavior for_userc
#
user-profile usera
 qos apply policy for_usera inbound
user-profile userb
 qos apply policy for_userb inbound
user-profile userc
 qos apply policy for_userc inbound
```

Control plane protection configuration examples

This chapter provides control plane protection configuration examples.

The units at the control plane are processing units that run most routing and switching protocols. Control plane units are responsible for protocol packet resolution and calculation, such as CPUs. Compared to data plane units, the control plane units allow for greater packet processing flexibility but have lower throughput.

Example: Configuring control plane protection

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

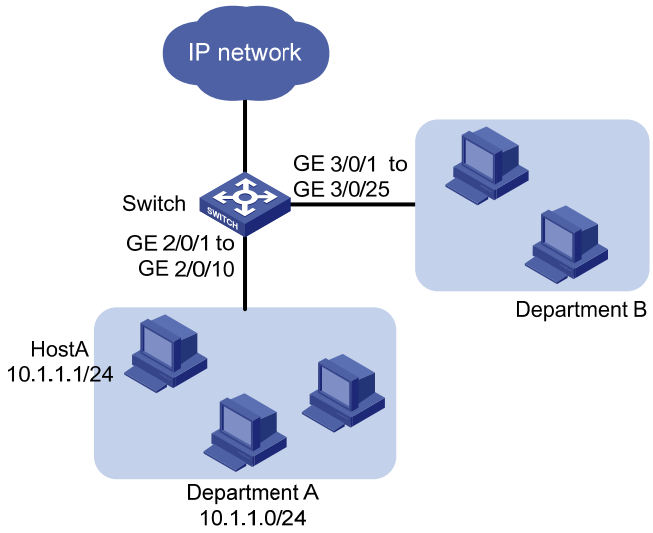
Network requirements

As shown in Figure 188, Switch, which is a distributed device, uses multiple ports on different interface cards to connect the two departments of the company.

Apply a QoS policy to the control plane to protect it as follows:

- In department A, limit the rate to 64 kbps for Telnet traffic from any host except Host A to Switch.
- Perform no limit on the rate of Telnet traffic from Host A to Switch.
- Limit the rate to 192 kbps for the ARP requests from Switch to department B.
- Perform no process for the excess ARP requests.
- Collect statistics about the processed ARP packets to avoid ARP request attacks against Switch.

Figure 188 Network diagram



Requirements analysis

The network requirements are analyzed as follows:

- Configure advanced ACLs to match Telnet protocol packets because the switch does not pre-define match criteria for Telnet packets. Configure traffic policing actions to rate-limit packets.
- A QoS policy is a set of class-behavior associations that are matched in the order that they are configured. You can use this feature to configure exceptional handling (not rate limiting) for the Telnet packets from Host A in the following workflow:
  a. Perform the following configurations:
     – Create a class to match the Telnet packets from Host A.
     – Configure a behavior to permit packets to pass through.
     – Associate the class with the behavior in the QoS policy.
  b. Perform the following configurations:
     – Create a class to match the Telnet packets from network segment 10.1.1.0/24.
     – Configure a behavior to perform traffic policing for packets.
     – Associate the class with the behavior in the QoS policy.

  Then, when the Telnet packets from Host A reaches Switch, they match the first class-behavior association and they pass through the switch, instead of proceeding to match the second class-behavior association.
- Because the switch has pre-defined match criteria for ARP packets, to rate limit and collect statistic about ARP packets, you can perform the following configurations:
  - Use the pre-defined system index-based match criteria for ARP packets in a class.
  - Associate the class with a behavior containing a traffic policing action and traffic accounting action.

Configuration restrictions and guidelines

When you configure control plane protection, follow these restrictions and guidelines:

- In a control plane QoS policy, a class using a system index-based match criterion can be associated with only a behavior containing traffic policing, traffic accounting, or both actions. Only the CIR configured for the traffic policing action applies.
- If the QoS policy applied to a control plane does not use the system index as the match criteria, the QoS actions in the QoS policy also take effect on the data traffic of the card where the control plane resides.

Configuration procedures

Configuring a control plane policy for the Telnet protocol

Configure IPv4 advanced ACL 3000 to match the Telnet protocol packets sourced from Host A.

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit tcp source 10.1.1.1 0 destination-port eq telnet
[Switch-acl-adv-3000] quit
```

Configure IPv4 advanced ACL 3001 to match the Telnet protocol packets sourced from network segment 10.1.1.0/24.

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination-port eq telnet
[Switch-acl-adv-3001] quit
```

Create a class named **host_a**, and use IPv4 ACL 3000 as the match criterion.

```
[Switch] traffic classifier host_a
[Switch-classifier-host_a] if-match acl 3000
[Switch-classifier-host_a] quit
```

Create traffic behavior **host_a**, and configure an action of permitting packets to pass through in the behavior.

```
[Switch] traffic behavior host_a
[Switch-behavior-host_a] filter permit
[Switch-behavior-host_a] quit
```

Create a class named **dept_a**, and use IPv4 ACL 3001 as the match criterion.

```
[Switch] traffic classifier dept_a
[Switch-classifier-dept_a] if-match acl 3001
[Switch-classifier-dept_a] quit
```

Create a traffic behavior named **dept_a**, and configure an action of rate limiting packets to 64 kbps in the behavior.

```
[Switch] traffic behavior dept_a
[Switch-behavior-dept_a] car cir 64
[Switch-behavior-dept_a] quit
```

Create a QoS policy named **for_telnet**.

```
[Switch] qos policy for_telnet
```

Associate class **host_a** with behavior **host_a**.

```
[Switch-qospolicy-for_telnet] classifier host_a behavior host_a
```

Associate class **dept_a** with behavior **dept_a**.

```
[Switch-qospolicy-for_telnet] classifier dept_a behavior dept_a
[Switch-qospolicy-for_telnet] quit
```

Apply QoS policy **for_telnet** to the incoming traffic of the control plane of the card in slot 2.

```
[Switch] control-plane slot 2
[Switch-cp-slot2] qos apply policy for_telnet inbound
[Switch-cp-slot2] quit
```

Configuring a control plane policy for the ARP protocol

Use the **display qos policy control-plane pre-defined** command to display the pre-defined system index-based policies on the card in slot 3.

```
[Switch] display qos policy control-plane pre-defined slot 3
```

```
=====================================================================
 Pre-defined Control-plane Policy Slot 3
---------------------------------------------------------------------
  Index |   PacketType              |  Priority  |  BandWidth(Kbps)
---------------------------------------------------------------------
  1          ISIS                          5           256
  29         ARP                           2           256
  30         ARP_REPLY                     3           256
  35         DOT1X                         2           128
  36         STP                           6           256
  37         LACP                          6           64
  38         GVRP                          3           64
  41         ICMP                          1           512
  53         LLDP                          4           64
  54         DLDP                          4           64
  106        IPV6_CPUDST_CAR               3           256
=====================================================================
```

The output shows that the system-index for ARP request is 29, and the pre-defined rate limit is 256 kbps.

NOTE:

The pre-defined system indexes for protocols vary by device model and software version. Make the following configurations based on the pre-defined system indexes on your switch.

Create a class named **for_arp**, and use system index 29 as the match criterion.

```
[Switch] traffic classifier for_arp
[Switch-classifier-for_arp] if-match system-index 29
[Switch-classifier-for_arp] quit
```

Create a traffic behavior named **for_arp**, and configure an action of rate limiting packets to 192 kbps and a traffic accounting action in the behavior.

```
[Switch] traffic behavior for_arp
[Switch-behavior-for_arp] car cir 192
[Switch-behavior-for_arp] accounting
[Switch-behavior-for_arp] quit
```

Create a QoS policy named **for_arp**, and associate class **for_arp** with traffic behavior **for_arp** in the QoS policy.

```
[Switch] qos policy for_arp
[Switch-qospolicy-for_arp] classifier for_arp behavior for_arp
[Switch-qospolicy-for_arp] quit
```

Apply QoS policy **for_arp** to the incoming traffic of the control plane of the card in slot 3.

```
[Switch] control-plane slot 3
[Switch-cp-slot3] qos apply policy for_arp inbound
[Switch-cp-slot3] quit
```

Verifying the configuration

Display the control plane QoS policy information on the card in slot 2.

```
[Switch] display qos policy control-plane slot 2
Control-plane slot 2
  Direction: Inbound
  Policy: for_telnet
   Classifier: host_a
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: host_a
      Filter Enable: permit
   Classifier: dept_a
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: dept_a
      Committed Access Rate:
        CIR 64 (kbps), CBS 512 (byte), EBS 512 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
        Green : 0(Packets)
        Red   : 0(Packets)
```

Display the pre-defined control plane QoS policy information on the card in slot 3.

```
[Switch] display qos policy control-plane pre-defined slot 3
=====================================================================
 Pre-defined Control-plane Policy Slot 3
---------------------------------------------------------------------
  Index |   PacketType              |  Priority  |  BandWidth(Kbps)
---------------------------------------------------------------------
  1          ISIS                          5          256
  29         ARP                           2          192
  30         ARP_REPLY                     3          256
  35         DOT1X                         2          128
  36         STP                           6          256
  37         LACP                          6          64
  38         GVRP                          3          64
```

```
  41          ICMP                        1           512
  53          LLDP                        4           64
  54          DLDP                        4           64
  106         IPV6_CPUDST_CAR             3           256
==============================================================
```

The output shows the rate limit for ARP protocol packets becomes the user-defined 192 kbps.

Configuration files

```
#
acl number 3000
 rule 0 permit tcp source 10.1.1.1 0 destination-port eq telnet
acl number 3001
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq telnet
#
traffic classifier host_a operator and
 if-match acl 3000
traffic classifier for_arp operator and
 if-match system-index 29
traffic classifier dept_a operator and
 if-match acl 3001
#
traffic behavior host_a
 filter permit
traffic behavior for_arp
 car cir 192 cbs 512 ebs 512 green pass red discard yellow pass
 accounting
traffic behavior dept_a
 car cir 64 cbs 512 ebs 512 green pass red discard yellow pass
#
qos policy for_telnet
 classifier host_a behavior host_a
 classifier dept_a behavior dept_a
qos policy for_arp
 classifier for_arp behavior for_arp
#
control-plane slot 2
 qos apply policy for_telnet inbound
control-plane slot 3
 qos apply policy for_arp inbound
```

QoS policy-based routing configuration examples

This chapter provides QoS policy-based routing configuration examples.

QoS policy-based routing uses user-defined policies to route packets. Policy-based routing takes precedence over traditional routing protocols. When the device forwards a packet, the device first matches the packet against the match criteria of policy-based routing. If a match is found, the packet is forwarded based on policy-based routing. Otherwise, the packet is forwarded based on traditional routing.

Example: Configuring QoS policy-based IPv4 routing

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

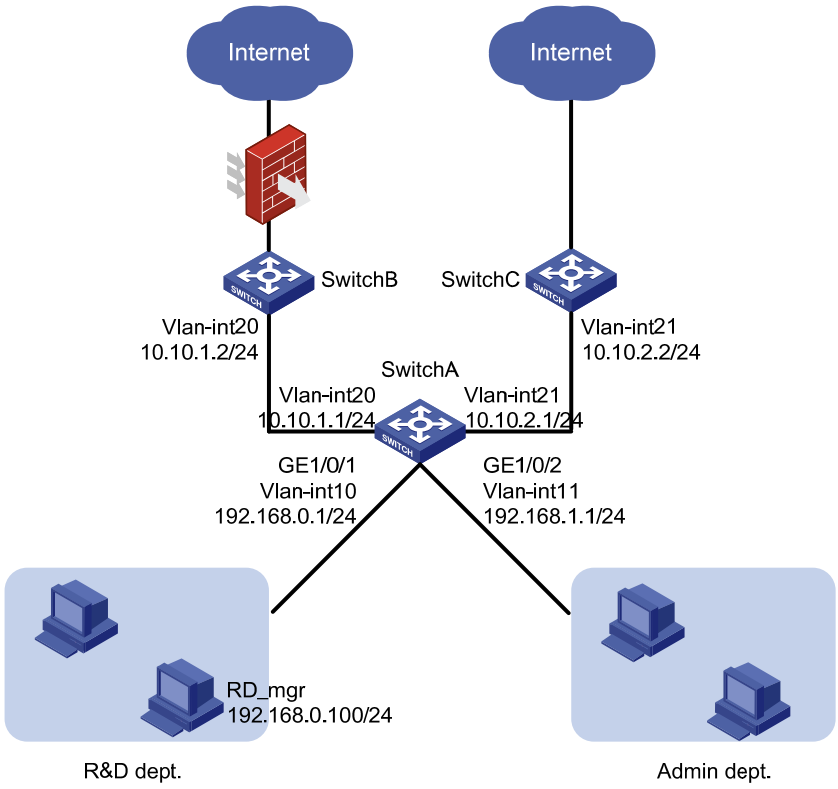
Network requirements

As shown in Figure 189, a company accesses the Internet through two SP networks. The Administration department and the R&D department of the company need to access the Internet.

To protect the information of the R&D department, configure the R&D department to access the specified websites in the Internet through the uplink of Switch B. Configure the firewall to filter and log the website access. The Administration department can access the Internet through Switch C without any restriction.

The host of the R&D department manager, with the IP address 192.168.0.100, can access the Internet through Switch C without any restrictions.

Figure 189 Network diagram



Requirements analysis

The network requirements are analyzed as follows:

- To forward packets with different characteristics along different paths, you can perform the following configurations:
  - Configure classes to classify packets by source IP address.
  - Configure actions of redirecting traffic to next hops in traffic behaviors.
  - Associate the classes with behaviors.
- The class-behavior associations in a QoS policy take effect in the order that they are configured. Therefore, you must configure the class-behavior association for the R&D department manager before you configure the class-behavior association for the whole network segment of the R&D department. Otherwise, the configuration for the R&D department manager fails.

Configuration restrictions and guidelines

Before you configure QoS policy-based routing, make sure all devices can reach other through traditional routing protocols.

Configuration procedures

Configuring routing protocols

Configure VLAN-interfaces and assign IP addresses to VLAN-interfaces on these devices, as shown in Figure 189. (Details not shown.)

Configure OSPF on Switch A to advertise the directly connected networks of Switch A.

```
<SwitchA> system-view
[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] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.10.2.0 0.0.0.255
```

Configure OSPF on Switch B to advertise the directly connected networks of Switch B.

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
```

Configure OSPF on Switch C to advertise the directly connected networks of Switch C.

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.10.2.0 0.0.0.255
```

Perform the following configurations:

- Configure the default gateway address as 192.168.0.1 for the hosts of the R&D department.
- Configure the default gateway address as 192.168.1.1 for the hosts in the Administration department.

After completing the preceding configuration, check whether each department can reach Switch B and Switch C. If they can, the routing protocols are correctly configured, and you can proceed with the following configurations.

Configuring QoS policy-based routing

Configure basic ACL 2000 to match the traffic with source IP address 192.168.0.0/24.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 192.168.0.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

Configure basic ACL 2001 to match the traffic with source IP address 192.168.1.0/24.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[SwitchA-acl-basic-2001] quit
```

Configure basic ACL 2002 to match the traffic with source IP address 192.168.0.100 (IP address of the R&D department manager's host).

```
[SwitchA] acl number 2002
[SwitchA-acl-basic-2002] rule permit source 192.168.0.100 0.0.0.0
[SwitchA-acl-basic-2002] quit
```

Create class **rd_internet**, and use ACL 2000 as the match criterion of the class.

```
[SwitchA] traffic classifier rd_internet
[SwitchA-classifier-rd_internet] if-match acl 2000
[SwitchA-classifier-rd_internet] quit
```

Create a behavior named **rd_internet**, and configure the action of redirecting traffic to Switch B (10.10.1.2) for the behavior.

```
[SwitchA] traffic behavior rd_internet
[SwitchA-behavior-rd_internet] redirect next-hop 10.10.1.2
[SwitchA-behavior-rd_internet] quit
```

Create class **admin_internet**, and use ACL 2001 as the match criterion of the class.

```
[SwitchA] traffic classifier admin_internet
[SwitchA-classifier-admin_internet] if-match acl 2001
[SwitchA-classifier-admin_internet] quit
```

Create a behavior named **admin_internet**, and configure the action of redirecting traffic to Switch C (10.10.2.2) for the behavior.

```
[SwitchA] traffic behavior admin_internet
[SwitchA-behavior-admin_internet] redirect next-hop 10.10.2.2
[SwitchA-behavior-admin_internet] quit
```

Create class **rd_mgr_internet**, and use ACL 2002 as the match criterion of the class.

```
[SwitchA] traffic classifier rd_mgr_internet
[SwitchA-classifier-rd_mgr_internet] if-match acl 2002
[SwitchA-classifier-rd_mgr_internet] quit
```

Use the traffic behavior **admin_internet** for the host of the R&D department manager.

Perform the following configurations:

- Create a QoS policy named **rd_internet**.
- Associate class **rd_mgr_internet** with traffic behavior **admin_internet**.
- Associate class **rd_internet** with traffic behavior **rd_internet**.

You must associate class **rd_mgr_internet** with traffic behavior **admin_internet** before associating class **rd_internet** with traffic behavior **rd_internet**.

```
[SwitchA] qos policy rd_internet
[SwitchA-qospolicy-rd_internet] classifier rd_mgr_internet behavior admin_internet
[SwitchA-qospolicy-rd_internet] classifier rd_internet behavior rd_internet
[SwitchA-qospolicy-rd_internet] quit
```

Create a QoS policy named **admin_internet**, and associate class **admin_internet** with traffic behavior **admin_internet**.

```
[SwitchA] qos policy admin_internet
[SwitchA-qospolicy-admin_internet] classifier admin_internet behavior admin_internet
[SwitchA-qospolicy-admin_internet] quit
```

Apply the QoS policy **rd_internet** to the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy rd_internet inbound
[SwitchA-GigabitEthernet1/0/1] quit
```

Apply the QoS policy **admin_internet** to the incoming traffic of GigabitEthernet 1/0/2.

```
[SwitchA] interface gigabitethernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] qos apply policy admin_internet inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about QoS policies applied to ports.

```
[SwitchA] display qos policy interface
Interface: GigabitEthernet1/2/0/2

  Direction: Inbound

  Policy: rd_internet
   Classifier: rd_mgr_internet
     Operator: AND
     Rule(s) : If-match acl 2002
     Behavior: admin_internet
      Redirect enable:
        Redirect type: next-hop
        Redirect destination:
          10.10.2.2
        Redirect fail-action: forward
   Classifier: rd_internet
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: rd_internet
      Redirect enable:
        Redirect type: next-hop
        Redirect destination:
          10.10.1.2
        Redirect fail-action: forward

  Interface: GigabitEthernet1/2/0/3

  Direction: Inbound

  Policy: admin_internet
   Classifier: admin_internet
     Operator: AND
     Rule(s) : If-match acl 2001
     Behavior: admin_internet
      Redirect enable:
        Redirect type: next-hop
        Redirect destination:
          10.10.2.2
        Redirect fail-action: forward
```

Configuration files

This section provides only the configuration files on Switch A. Only routing protocols need to be configured on Switch B and Switch C. Their configuration files are not provided.

```
#
acl number 2000
 rule 0 permit source 192.168.0.0 0.0.0.255
acl number 2001
 rule 0 permit source 192.168.1.0 0.0.0.255
acl number 2002
 rule 0 permit source 192.168.0.100 0
#
traffic classifier admin_internet operator and
 if-match acl 2001
traffic classifier rd_mgr_internet operator and
 if-match acl 2002
traffic classifier rd_internet operator and
 if-match acl 2000
#
traffic behavior admin_internet
 redirect next-hop 10.10.2.2 fail-action forward
traffic behavior rd_internet
 redirect next-hop 10.10.1.2 fail-action forward
#
qos policy admin_internet
 classifier admin_internet behavior admin_internet
qos policy rd_internet
 classifier rd_mgr_internet behavior admin_internet
 classifier rd_internet behavior rd_internet
#
interface GigabitEthernet1/0/1
 qos apply policy rd_internet inbound
#
interface GigabitEthernet1/0/2
 qos apply policy admin_internet inbound
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
```

Example: Configuring QoS policy-based IPv6 routing

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 190, a company accesses the Internet through two SP networks. The Administration department and the R&D department of the company need to access the Internet.

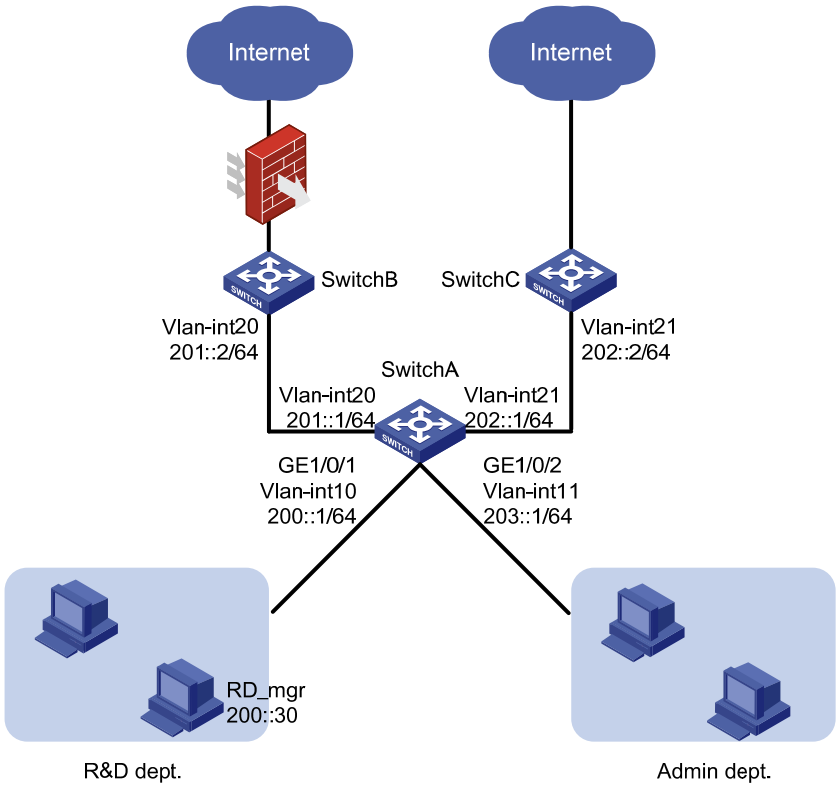
To protect the information of the R&D department, perform the following configurations:

- Configure the R&D department to access the specified websites in the Internet through the uplink of Switch B.
- Configure the firewall to filter and log the website access.

The Administration department can access the Internet through Switch C without any restrictions.

The host of the R&D department manager, with the IPv6 address 200::30, can access the Internet through Switch C without any restrictions.

Figure 190 Network diagram



Requirements analysis

To forward packets with different characteristics along different paths, you can perform the following configurations:

- Configure classes to classify packets by source IP address.
- Configure actions of redirecting traffic to next hops in traffic behaviors.
- Associate the classes with behaviors.

The class-behavior associations in a QoS policy take effect in the order that they are configured. Therefore, you must configure the class-behavior association for the R&D department manager before you configure the class-behavior association for the whole network segment of the R&D department. Otherwise, the configuration for the R&D department manager fails.

Configuration restrictions and guidelines

Before you configure QoS policy-based routing, make sure all devices can reach other through traditional routing protocols.

Configuration procedures

Configuring routing protocols

Configure VLAN interfaces and assign IP addresses to VLAN-interfaces on these devices, as shown in Figure 190. (Details not shown.)

Enable RIPng on Switch A, and enable RIPng on each VLAN interface on Switch A.

```
<SwitchA> system-view
[SwitchA] ripng
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ripng 1 enable
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ripng 1 enable
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ripng 1 enable
[SwitchA] interface vlan-interface 21
[SwitchA-Vlan-interface21] ripng 1 enable
```

Enable RIPng on Switch B, and enable RIPng on VLAN-interface 20.

```
<SwitchB> system-view
[SwitchB] ripng
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] ripng 1 enable
```

Enable RIPng on Switch C, and enable RIPng on VLAN-interface 21.

```
<SwitchC> system-view
[SwitchC] ripng
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 21
[SwitchC-Vlan-interface21] ripng 1 enable
```

Perform the following configurations:

- Configure the default gateway address as 200::1/64 for the hosts of the R&D department.
- Configure the default gateway address as 203::1/64 for the hosts in the Administration department.

After completing the preceding configuration, check whether each department can reach Switch B and Switch C. If they can, the routing protocols are correctly configured, and you can proceed with the following configurations.

Configuring QoS policy-based routing

Configure IPv6 basic ACL 2000 to match the traffic with source IP address 200::0/64.

```
[SwitchA] acl ipv6 number 2000
[SwitchA-acl6-basic-2000] rule permit source 200::0 64
[SwitchA-acl6-basic-2000] quit
```

Configure IPv6 basic ACL 2001 to match the traffic with source IP address 203::0/64.

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source 203::0 64
[SwitchA-acl6-basic-2001] quit
```

Configure IPv6 basic ACL 2002 to match the traffic with source IP address 200::30/128 (IP address of the R&D department manager's host).

```
[SwitchA] acl ipv6 number 2002
[SwitchA-acl6-basic-2002] rule permit source 200::30 128
[SwitchA-acl6-basic-2002] quit
```

Create class **rd_internet**, and use IPv6 ACL 2000 as the match criterion of the class.

```
[SwitchA] traffic classifier rd_internet
[SwitchA-classifier-rd_internet] if-match acl ipv6 2000
[SwitchA-classifier-rd_internet] quit
```

Create a behavior named **rd_internet**, and configure the action of redirecting traffic to Switch B (201::2) for the behavior.

```
[SwitchA] traffic behavior rd_internet
[SwitchA-behavior-rd_internet] redirect next-hop 201::2
[SwitchA-behavior-rd_internet] quit
```

Create class **admin_internet**, and use IPv6 ACL 2001 as the match criterion of the class.

```
[SwitchA] traffic classifier admin_internet
[SwitchA-classifier-admin_internet] if-match acl ipv6 2001
[SwitchA-classifier-admin_internet] quit
```

Create a behavior named **admin_internet**, and configure the action of redirecting traffic to Switch C (202::2) for the behavior.

```
[SwitchA] traffic behavior admin_internet
[SwitchA-behavior-admin_internet] redirect next-hop 202::2
[SwitchA-behavior-admin_internet] quit
```

Create class **rd_mgr_internet**, and use IPv6 ACL 2002 as the match criterion of the class.

```
[SwitchA] traffic classifier rd_mgr_internet
[SwitchA-classifier-rd_mgr_internet] if-match acl ipv6 2002
[SwitchA-classifier-rd_mgr_internet] quit
```

Use the traffic behavior **admin_internet** for the host of the R&D department manager.

Perform the following configurations:

- Create a QoS policy named **rd_internet**.
- Associate class **rd_mgr_internet** with traffic behavior **admin_internet**.
- Associate class **rd_internet** with traffic behavior **rd_internet**.

You must associate class **rd_mgr_internet** with traffic behavior **admin_internet** before associating class **rd_internet** with traffic behavior **rd_internet**.

```
[SwitchA] qos policy rd_internet
[SwitchA-qospolicy-rd_internet] classifier rd_mgr_internet behavior admin_internet
[SwitchA-qospolicy-rd_internet] classifier rd_internet behavior rd_internet
[SwitchA-qospolicy-rd_internet] quit
```

Create a QoS policy named **admin_internet**, and associate class **admin_internet** with traffic behavior **admin_internet**.

```
[SwitchA] qos policy admin_internet
[SwitchA-qospolicy-admin_internet] classifier admin_internet behavior admin_internet
[SwitchA-qospolicy-admin_internet] quit
```

Apply the QoS policy **rd_internet** to the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy rd_internet inbound
[SwitchA-GigabitEthernet1/0/1] quit
```

Apply the QoS policy **admin_internet** to the incoming traffic of GigabitEthernet 1/0/2.

```
[SwitchA] interface gigabitethernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] qos apply policy admin_internet inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about QoS policies applied to ports.

```
[SwitchA] display qos policy interface

Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: admin_internet
   Classifier: admin_internet
     Operator: AND
     Rule(s) : If-match acl 2001
               If-match acl ipv6 2001
     Behavior: admin_internet
      Redirect enable:
        Redirect type: next-hop
        Redirect destination:
          202::2
        Redirect fail-action: forward

  Interface: GigabitEthernet1/0/2

  Direction: Inbound

  Policy: admin_internet
   Classifier: admin_internet
     Operator: AND
     Rule(s) : If-match acl 2001
               If-match acl ipv6 2001
     Behavior: admin_internet
      Redirect enable:
        Redirect type: next-hop
        Redirect destination:
          202::2
        Redirect fail-action: forward
```

Configuration files

```
#
acl ipv6 number 2000
 rule 0 permit source 200::/64
acl ipv6 number 2001
 rule 0 permit source 203::/64
acl ipv6 number 2002
```

```
 rule 0 permit source 200::30/128
#
traffic classifier admin_internet operator and
 if-match acl ipv6 2001
traffic classifier rd_mgr_internet operator and
 if-match acl ipv6 2002
traffic classifier rd_internet operator and
 if-match acl ipv6 2000
#
traffic behavior admin_internet
 redirect next-hop 202::2 fail-action forward
traffic behavior rd_internet
 redirect next-hop 201::2 fail-action forward
#
qos policy admin_internet
 classifier admin_internet behavior admin_internet
qos policy rd_internet
 classifier rd_mgr_internet behavior admin_internet
 classifier rd_internet behavior rd_internet
#
interface Vlan-interface10
 ripng 1 enable
#
interface Vlan-interface11
 ripng 1 enable
#
interface Vlan-interface20
 ripng 1 enable
#
interface Vlan-interface21
 ripng 1 enable
#
interface GigabitEthernet1/0/1
 qos apply policy rd_internet inbound
#
interface GigabitEthernet1/0/2
 qos apply policy admin_internet inbound
#
ripng 1
#
```

Configuration examples for implementing HQoS through marking local QoS IDs

This chapter provides examples for implementing HQoS through marking local QoS IDs.

The local QoS ID marking function allows you to reclassify the packets that match multiple match criteria and then configure traffic behaviors for the reclassified packets.

Example: Configuring HQoS through marking local QoS IDs

Applicable product matrix

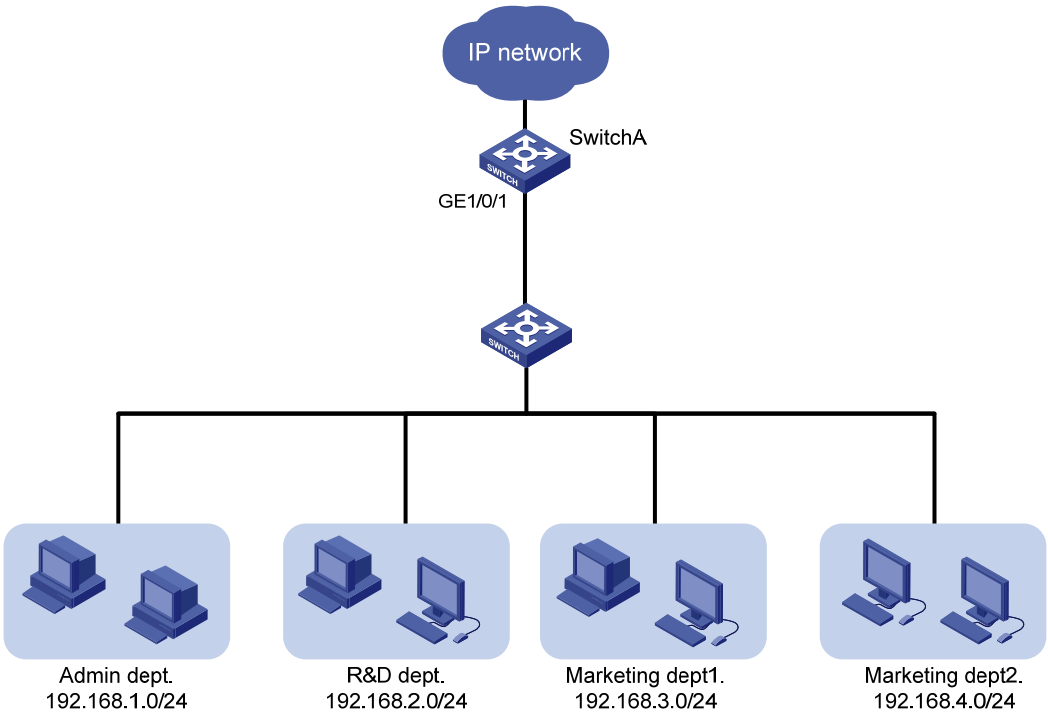
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 191, configure traffic policing and local QoS ID marking to limit the rate of traffic that accesses the IP network, as follows:

- Limit the rate of traffic from the Administration department and the rate of traffic from the R&D department to 1024 kbps each.
- Limit the rate of traffic from the Marketing department, which has two sub-departments, to 2048 kbps.

Figure 191 Network diagram



Configuration restrictions and guidelines

Class-behavior associations take effect in the order that they are configured. When you configure a QoS policy, you must first configure the class-behavior association for marking a local QoS ID. Then configure class-behavior association for performing actions for traffic that matches the local QoS ID.

Configuration procedures

Limiting the uplink traffic of the Administration department and the R&D department

Configure IPv4 basic ACL 2001 to match the traffic from the Administration department.

```
<SwitchA> system-view
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[SwitchA-acl-basic-2001] quit
```

Configure IPv4 basic ACL 2002 to match the traffic from the R&D department.

```
[SwitchA] acl number 2002
[SwitchA-acl-basic-2002] rule permit source 192.168.2.0 0.0.0.255
[SwitchA-acl-basic-2002] quit
```

Configure traffic class **admin** to match the traffic from the Administration department.

```
[SwitchA] traffic classifier admin
[SwitchA-classifier-admin] if-match acl 2001
[SwitchA-classifier-admin] quit
```

Configure traffic class **rd** to match the traffic from the R&D department.

```
[SwitchA] traffic classifier rd
```

```
[SwitchA-classifier-rd] if-match acl 2002
[SwitchA-classifier-rd] quit
```

Create a behavior named **car_admin_rd**, and configure a CAR action for the behavior as follows: set the CIR to 1024 kbps.

```
[SwitchA] traffic behavior car_admin_rd
[SwitchA-behavior-car_admin_rd] car cir 1024
[SwitchA-behavior-car_admin_rd] quit
```

Create a QoS policy named **car**, and associate traffic class **admin** and traffic class **rd** with traffic behavior **car_admin_rd** in the QoS policy.

```
[SwitchA] qos policy car
[SwitchA-qospolicy-car] classifier admin behavior car_admin_rd
[SwitchA-qospolicy-car] classifier rd behavior car_admin_rd
[SwitchA-qospolicy-car] quit
```

Limiting the uplink traffic of the Marketing department

Configure IPv4 basic ACL 2003 to match traffic from Marketing department 1.

```
[SwitchA] acl number 2003
[SwitchA-acl-basic-2003] rule permit source 192.168.3.0 0.0.0.255
[SwitchA-acl-basic-2003] quit
```

Configure IPv4 basic ACL 2004 to match the traffic from Marketing department 2.

```
[SwitchA] acl number 2004
[SwitchA-acl-basic-2004] rule permit source 192.168.4.0 0.0.0.255
[SwitchA-acl-basic-2004] quit
```

Create a class named **marketing**, and configure the class to match traffic from Marketing department 1 and Marketing department 2.

```
[SwitchA] traffic classifier marketing operator or
[SwitchA-classifier-marketing] if-match acl 2003
[SwitchA-classifier-marketing] if-match acl 2004
[SwitchA-classifier-marketing] quit
```

Create a behavior named **remark_local_id**, and configure the action of marking traffic with local QoS ID 100 for the behavior.

```
[SwitchA] traffic behavior remark_local_id
[SwitchA-behavior-remark_local_id] remark qos-local-id 100
[SwitchA-behavior-remark_local_id] quit
```

Create a class named **marketing_car**, and configure the class to mark traffic from Marketing department 1 or Marketing department 2. The traffic is marked with local QoS ID 100.

```
[SwitchA] traffic classifier marketing_car
[SwitchA-classifier-marketing_car] if-match qos-local-id 100
[SwitchA-classifier-marketing_car] quit
```

Create a behavior named **marketing_car**, and configure a CAR action for the behavior as follows: set the CIR to 2048 kbps.

```
[SwitchA] traffic behavior marketing_car
[SwitchA-behavior-marketing_car] car cir 2048
[SwitchA-behavior-marketing_car] quit
```

In QoS policy named **car**, associate traffic class **marketing** with traffic behavior **remark_local_id** to mark the traffic from the Marketing department with local QoS ID 100.

```
[SwitchA] qos policy car
[SwitchA-qospolicy-car] classifier marketing behavior remark_local_id
```

Associate traffic class **marketing_car** with traffic behavior **marketing_car** to perform traffic policing for traffic marked with local QoS ID 100.

```
[SwitchA-qospolicy-car] classifier marketing_car behavior marketing_car
[SwitchA-qospolicy-car] quit
```

Apply QoS policy **car** to the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy car inbound
```

Verifying the configuration

Display information about QoS policies applied to GigabitEthernet 1/0/1.

```
[SwitchA] display qos policy interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: car
   Classifier: admin
     Operator: AND
     Rule(s) : If-match acl 2001
     Behavior: car_admin_rd
      Committed Access Rate:
        CIR 1024 (kbps), CBS 64000 (byte), EBS 512 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
        Green : 0(Packets)
        Red   : 0(Packets)
   Classifier: rd
     Operator: AND
     Rule(s) : If-match acl 2002
     Behavior: car_admin_rd
      Committed Access Rate:
        CIR 1024 (kbps), CBS 64000 (byte), EBS 512 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
        Green : 0(Packets)
        Red   : 0(Packets)
   Classifier: marketing
     Operator: OR
     Rule(s) : If-match acl 2003
               If-match acl 2004
     Behavior: remark_local_id
      Marking:
```

```
        Remark qos local ID 100
   Classifier: marketing_car
     Operator: AND
     Rule(s) : If-match qos-local-id 100
     Behavior: marketing_car
      Committed Access Rate:
        CIR 2048 (kbps), CBS 128000 (byte), EBS 512 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
        Green : 0(Packets)
        Red   : 0(Packets)
```

Configuration files

```
#
acl number 2001
 rule 0 permit source 192.168.1.0 0.0.0.255
acl number 2002
 rule 0 permit source 192.168.2.0 0.0.0.255
acl number 2003
 rule 0 permit source 192.168.3.0 0.0.0.255
acl number 2004
 rule 0 permit source 192.168.4.0 0.0.0.255
#
traffic classifier marketing operator or
 if-match acl 2003
 if-match acl 2004
traffic classifier marketing_car operator and
 if-match qos-local-id 100
traffic classifier rd operator and
 if-match acl 2002
traffic classifier admin operator and
 if-match acl 2001
#
traffic behavior car_admin_rd
 car cir 1024 cbs 64000 ebs 512 green pass red discard yellow pass
traffic behavior marketing_car
 car cir 2048 cbs 128000 ebs 512 green pass red discard yellow pass
traffic behavior remark_local_id
 remark qos-local-id 100
#
qos policy car
 classifier admin behavior car_admin_rd
 classifier rd behavior car_admin_rd
 classifier marketing behavior remark_local_id
 classifier marketing_car behavior marketing_car
#
```

```
interface GigabitEthernet1/0/1
 qos apply policy car inbound
```

RRPP configuration examples

This chapter provides RRPP configuration examples.

RRPP can do the following:

- Prevents broadcast storms caused by data loops when an Ethernet ring is healthy.
- Rapidly restores the communication paths between the nodes in the event that a link is disconnected on the ring.

General configuration restrictions and guidelines

When you configure RRPP, follow these restrictions and guidelines:

- To ensure proper forwarding of RRPPDUs, do not enable 802.1Q in 802.1Q (QinQ) or VLAN mapping on the control VLANs.
- RRPP ports must be Layer-2 Ethernet ports or Layer-2 aggregate interfaces. The Layer-2 Ethernet ports cannot be member ports of any Layer-2 aggregation group, service loopback group, or smart link group.
- You must disable the spanning tree feature on the ports connected to an RRPP ring. Do not enable Smart Link on the ports.
- Do not configure a port connected to an RRPP ring as the monitor port of a mirroring group.
- To accelerate topology convergence, HP recommends canceling the physical state change suppression interval setting on a port that is not connected to an RRPP ring.

Example: Configuring single ring

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

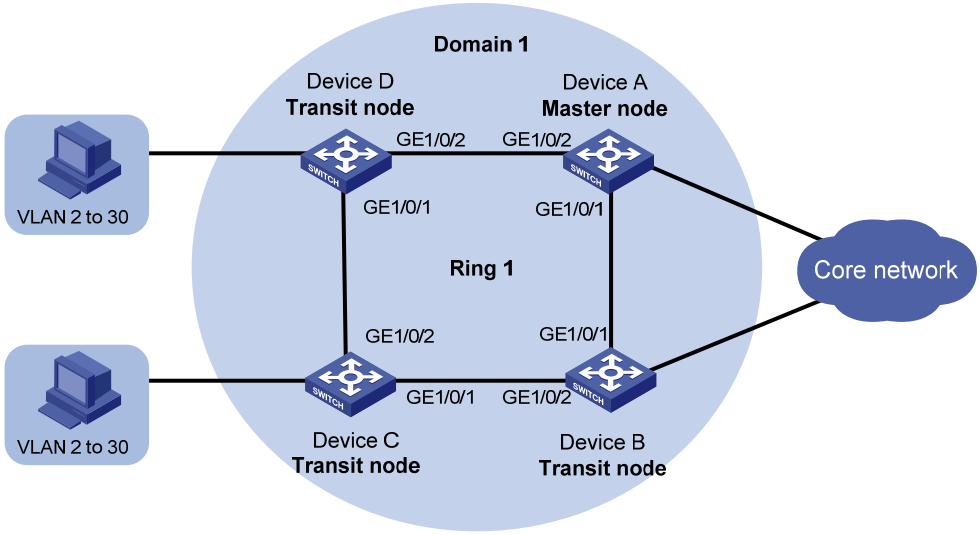
As shown in Figure 192, multiple users are connected to the distribution-layer network that adopts an RRPP ring topology.

Configure RRPP to meet the following requirements:

- When all physical links on Ring 1 are connected, the nodes on the ring can communicate with each another, and no broadcast storms can occur due to data loops.
- When a physical link on Ring 1 is broken, RRPP immediately restores communication between the nodes to ensure convergence performance of the network.

- When the broken link is restored, the link can forward data traffic again, and no loops occur.

Figure 192 Network diagram



Requirements analysis

The master node initiates the polling mechanism and determines the operations to be performed after a change in topology. Therefore, you must configure a device with high performance as the master node. In this example, configure Device A as the master node.

Configuration restrictions and guidelines

When you configure single ring, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.

Configuration procedures

Configuring Device A

1. Create VLANs 2 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

1. Create VLANs 2 through 30.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 2 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C and Device D

Configure Device C and Device D in the same way Device B is configured. (Details not shown.)

Verifying the configuration

When all physical links on Ring 1 are connected, display detailed RRPP information about Ring 1.

```
<DeviceA> display rrpp verbose domain 1 ring 1
Domain ID     : 1
Control VLAN  : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer   : 1  sec  Fail Timer : 3  sec
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
Ring ID       : 1
Ring Level    : 0
```

```
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1                    Port status: UP
Secondary port: GE1/0/2                    Port status: BLOCKED
```

The output shows that all physical links on Ring 1 are connected. Interface GigabitEthernet 1/0/2 on Device A is blocked and cannot forward data packets.

Shut down GigabitEthernet 1/0/2 on Device B, and display detailed RRPP information about Ring 1 on Device A and Device B.

```
<DeviceA> display rrpp verbose domain 1 ring 1
Domain ID     : 1
Control VLAN  : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer   : 1  sec  Fail Timer : 3  sec
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Failed
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1                    Port status: UP
Secondary port: GE1/0/2                    Port status: UP
```

The output shows that a physical link on Ring 1 is broken. Interface GigabitEthernet 1/0/2 on Device A is up and can forward data packets.

```
<DeviceB> display rrpp verbose domain 1 ring 1
Domain ID     : 1
Control VLAN  : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer   : 1  sec  Fail Timer : 3  sec
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
Ring ID       : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : -
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1                    Port status: UP
Secondary port: GE1/0/2                    Port status: Down
```

The output shows that interface GigabitEthernet 1/0/2 on Device B is down.

Bring up GigabitEthernet 1/0/2 on Device B, and display detailed RRPP information about Ring 1 on Device A and Device B.

```
<DeviceA> display rrpp verbose domain 1 ring 1
Domain ID     : 1
Control VLAN  : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer   : 1  sec  Fail Timer : 3  sec
```

```
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1                    Port status: UP
Secondary port: GE1/0/2                    Port status: BLOCKED
```

The output shows that all physical links on Ring 1 are connected. Interface GigabitEthernet 1/0/2 on Device A is blocked and cannot forward data packets.

```
<DeviceB> display rrpp verbose domain 1 ring 1
Domain ID     : 1
Control VLAN  : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer   : 1  sec  Fail Timer : 3  sec
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
Ring ID       : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : -
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1                    Port status: UP
Secondary port: GE1/0/2                    Port status: UP
```

The output shows that interface GigabitEthernet 1/0/2 on Device B comes up again and can forward data packets.

Configuration files

- Device A:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
```

```
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B, Device C, and Device D:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

Example: Configuring intersecting ring

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

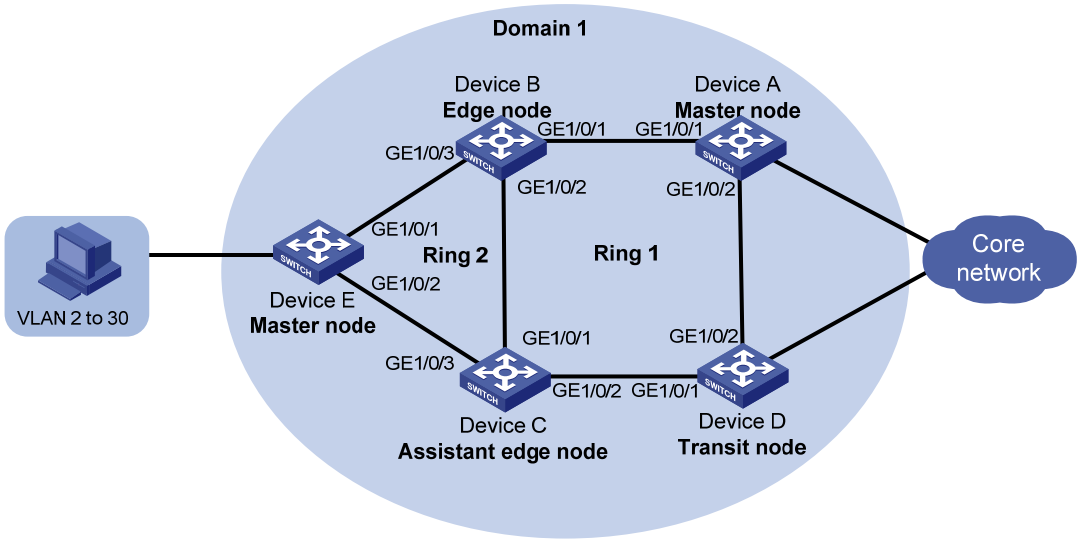
As shown in Figure 193:

- Device E at the access layer is connected to the distribution layer by using a ring topology.
- The distribution layer also adopts a ring topology.

Configure RRPP to meet the following requirements:

- When all physical links on Ring 1 or Ring 2 are connected, the nodes on the ring can communicate with each another, and no broadcast storms can occur due to data loops.
- When a physical link on Ring 1 or Ring 2 is broken, RRPP immediately restores communication between the nodes to ensure convergence performance of the network.
- When the broken link is restored, the link can forward data traffic again, and no loops occur.

Figure 193 Network diagram



Requirements analysis

The primary ring must feature high transmission capability for transparently transmitting traffic of the protected VLANs and control VLANs of the subrings. In this example, configure Ring 1 as the primary ring and Ring 2 as the subring.

For the primary ring, configure a device with high performance as the master node. For the subring, configure a device other than a common node as the master node. In this example, configure Device A as the master node of Ring 1 and Device B as the master node of Ring 2.

Configuration restrictions and guidelines

When you configure intersecting ring, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.

- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before enabling the subrings on their separate master nodes. On an edge node or assistant-edge node, enable the primary ring of an RRPP domain before enabling the subrings of the RRPP domain.

Configuration procedures

Configuring Device A

1. Create VLANs 2 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

1. Create VLANs 2 through 30.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 2 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/3] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device B as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 enable
```

Configure Device B as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
```

Enable ring 2.

```
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C

1. Create VLANs 2 through 30.

```
<DeviceC> system-view
[DeviceC] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 2 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
```

```
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/3] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceC] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceC-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device C as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 enable
```

   # Configure Device C as the assistant-edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet
1/0/3
```

   # Enable ring 2.

```
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit
```

   # Enable RRPP.

```
[DeviceC] rrpp enable
```

Configuring Device D

1. Create VLANs 2 through 30.

```
<DeviceD> system-view
[DeviceD] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 2 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceD] rrpp enable
```

Configuring Device E

1. Create VLANs 2 through 30.

```
<DeviceE> system-view
[DeviceE] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 2 to 30
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
```

```
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceE] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

   # Enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

   # Enable RRPP.

```
[DeviceE] rrpp enable
```

Verifying the configuration

Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "Example: Configuring single ring."

Configuration files

- Device A:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
```

```
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp enable
#
```

- Device C:

```
#
vlan 2 to 30
```

```
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp enable
#
```

- Device D:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
```

```
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device E:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 2 enable
#
rrpp enable
#
```

Example: Configuring dual homed rings

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

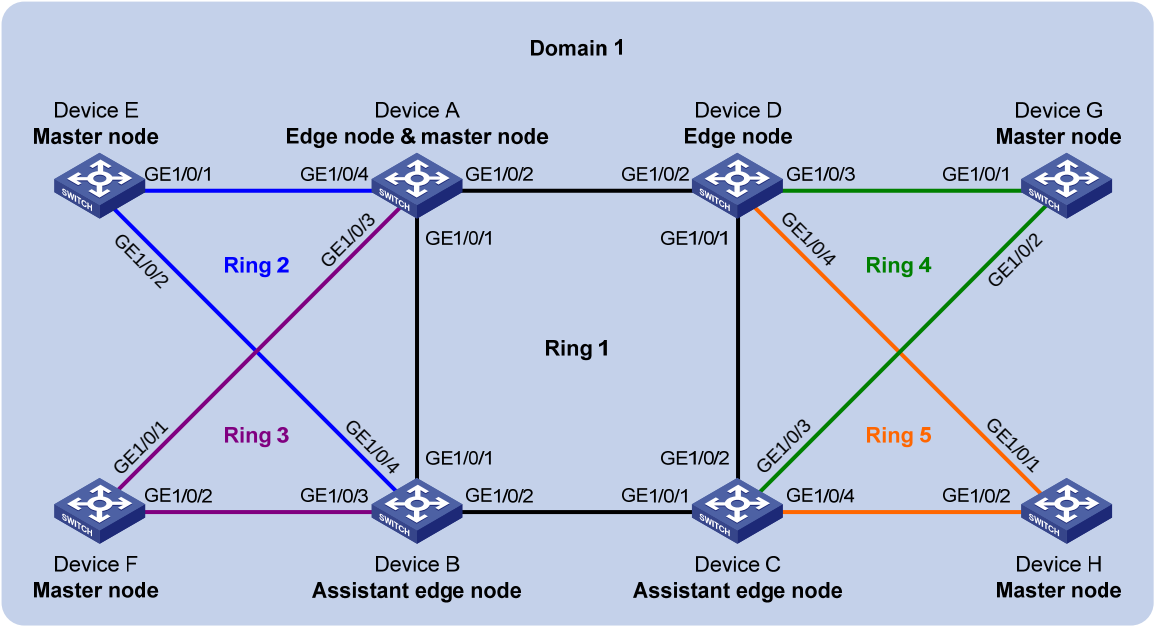
Network requirements

As shown in Figure 194, multiple access-layer devices are connected to the distribution layer by using a ring topology. The distribution layer also adopts a ring topology.

Configure RRPP to meet the following requirements:

- When all physical links on an Ethernet ring are connected, the nodes on the ring can communicate with each another, and no broadcast storms can occur due to data loops.
- When a physical link on an Ethernet ring is broken, RRPP immediately restores communication between the nodes to ensure convergence performance of the network.
- When the broken link is restored, the link can forward data traffic again, and no loops occur.

Figure 194 Network diagram



Requirements analysis

If multiple intersecting rings exist in an RRPP domain, configure the ring that connects all of them as the primary ring. In this example, configure Ring 1 as the primary ring and Ring 2 through Ring 5 as subrings.

For the primary ring, configure a device with high performance as the master node. For the subring, configure a device other than a common node as the master node. In this example:

- Configure Device A as the master node of Ring 1.
- Configure Device E, Device F, Device G, and Device H as the master node of Ring 2, Ring 3, Ring 4, and Ring 5, respectively.

Configuration restrictions and guidelines

When you configure dual homed rings, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.
- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before enabling the subrings on their separate master nodes. On an edge node or assistant-edge node, enable the primary ring of an RRPP domain before enabling the subrings of the RRPP domain.

Configuration procedures

Configuring Device A

1. Create VLANs 2 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
```

   # Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
```

   # Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
```

```
[DeviceA-GigabitEthernet1/0/4] undo stp enable
[DeviceA-GigabitEthernet1/0/4] port link-type trunk
[DeviceA-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/4] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 enable
```

   # Configure Device A as the edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port.

```
[DeviceA-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/4
```

   # Enable ring 2.

```
[DeviceA-rrpp-domain1] ring 2 enable
```

   # Configure Device A as the edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceA-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/3
```

   # Enable ring 3.

```
[DeviceA-rrpp-domain1] ring 3 enable
[DeviceA-rrpp-domain1] quit
```

   # Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

1. Create VLANs 2 through 30.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 2 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/4] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 enable
```

Configure Device B as the assistant-edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port.

```
[DeviceB-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet
1/0/4
```

Enable ring 2.

```
[DeviceB-rrpp-domain1] ring 2 enable
```

Configure Device B as the assistant-edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet
1/0/3
```

Enable ring 3.

```
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C

1. Create VLANs 2 through 30.

```
<DeviceC> system-view
[DeviceC] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 2 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo stp enable
```

```
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/4] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceC] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceC-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 enable
```

   # Configure Device C as the assistant-edge node of subring 4, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceC-rrpp-domain1] ring 4 node-mode assistant-edge edge-port gigabitethernet
1/0/3
```

   # Enable ring 4.

```
[DeviceC-rrpp-domain1] ring 4 enable
```

   # Configure Device C as the assistant-edge node of subring 5, with GigabitEthernet 1/0/4 as the edge port.

```
[DeviceC-rrpp-domain1] ring 5 node-mode assistant-edge edge-port gigabitethernet
1/0/4
```

   # Enable ring 5.

```
[DeviceC-rrpp-domain1] ring 5 enable
[DeviceC-rrpp-domain1] quit
```

   # Enable RRPP.

```
[DeviceC] rrpp enable
```

Configuring Device D

1. Create VLANs 2 through 30.

```
<DeviceD> system-view
[DeviceD] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 2 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD-GigabitEthernet1/0/2] quit
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD-GigabitEthernet1/0/3] quit
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] undo stp enable
[DeviceD-GigabitEthernet1/0/4] port link-type trunk
[DeviceD-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/4] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 enable
```

Configure Device D as the edge node of subring 4, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceD-rrpp-domain1] ring 4 node-mode edge edge-port gigabitethernet 1/0/3
```

Enable ring 4.

```
[DeviceD-rrpp-domain1] ring 4 enable
```

Configure Device D as the edge node of subring 5, with GigabitEthernet 1/0/4 as the edge port.

```
[DeviceD-rrpp-domain1] ring 5 node-mode edge edge-port gigabitethernet 1/0/4
```

Enable ring 5.

```
[DeviceD-rrpp-domain1] ring 5 enable
[DeviceD-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceD] rrpp enable
```

Configuring Device E

1. Create VLANs 2 through 30.

```
<DeviceE> system-view
[DeviceE] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 2 to 30
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceE] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

Enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceE] rrpp enable
```

Configuring Device F

1. Create VLANs 2 through 30.

```
<DeviceF> system-view
[DeviceF] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 2 to 30
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceF-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceF-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceF] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceF-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device F as the master node of subring 3, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

Enable ring 3.

```
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceF] rrpp enable
```

Configuring Device G

1. Create VLANs 2 through 30.

```
<DeviceG> system-view
[DeviceG] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceG] stp region-configuration
[DeviceG-mst-region] instance 1 vlan 2 to 30
[DeviceG-mst-region] active region-configuration
[DeviceG-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceG-GigabitEthernet1/0/1] port link-type trunk
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceG-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[DeviceG-GigabitEthernet1/0/2] port link-type trunk
[DeviceG-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceG-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceG] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceG-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceG-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device G as the master node of subring 4, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceG-rrpp-domain1] ring 4 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

Enable ring 4.

```
[DeviceG-rrpp-domain1] ring 4 enable
```

```
[DeviceG-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceG] rrpp enable
```

Configuring Device H

1. Create VLANs 2 through 30.

```
<DeviceH> system-view
[DeviceH] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceH] stp region-configuration
[DeviceH-mst-region] instance 1 vlan 2 to 30
[DeviceH-mst-region] active region-configuration
[DeviceH-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceH-GigabitEthernet1/0/1] port link-type trunk
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceH-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[DeviceH-GigabitEthernet1/0/2] port link-type trunk
[DeviceH-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceH-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceH] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceH-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceH-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device H as the master node of subring 5, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceH-rrpp-domain1] ring 5 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

Enable ring 5.

```
[DeviceH-rrpp-domain1] ring 5 enable
[DeviceH-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceH] rrpp enable
```

Verifying the configuration

Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "Example: Configuring single ring."

Configuration files

- Device A:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/4
 ring 2 enable
 ring 3 node-mode edge edge-port GigabitEthernet1/0/3
 ring 3 enable
#
```

```
rrpp enable
#
```

- Device B:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 2 enable
 ring 3 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 3 enable
#
rrpp enable
#
```

- Device C:

```
#
vlan 2 to 30
#
stp region-configuration
```

```
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 4 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 4 enable
 ring 5 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 5 enable
#
rrpp enable
#
```

- Device D:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
```

```
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 4 node-mode edge edge-port GigabitEthernet1/0/3
 ring 4 enable
 ring 5 node-mode edge edge-port GigabitEthernet1/0/4
 ring 5 enable
#
rrpp enable
#
```

- Device E:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
```

```
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 2 enable
#
rrpp enable
#
```

- Device F:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 3 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 3 enable
#
rrpp enable
#
```

- Device G:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
```

```
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 4 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 4 enable
#
rrpp enable
#
```

- Device H:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 5 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 5 enable
#
rrpp enable
#
```

Example: Configuring load balanced intersecting-ring

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

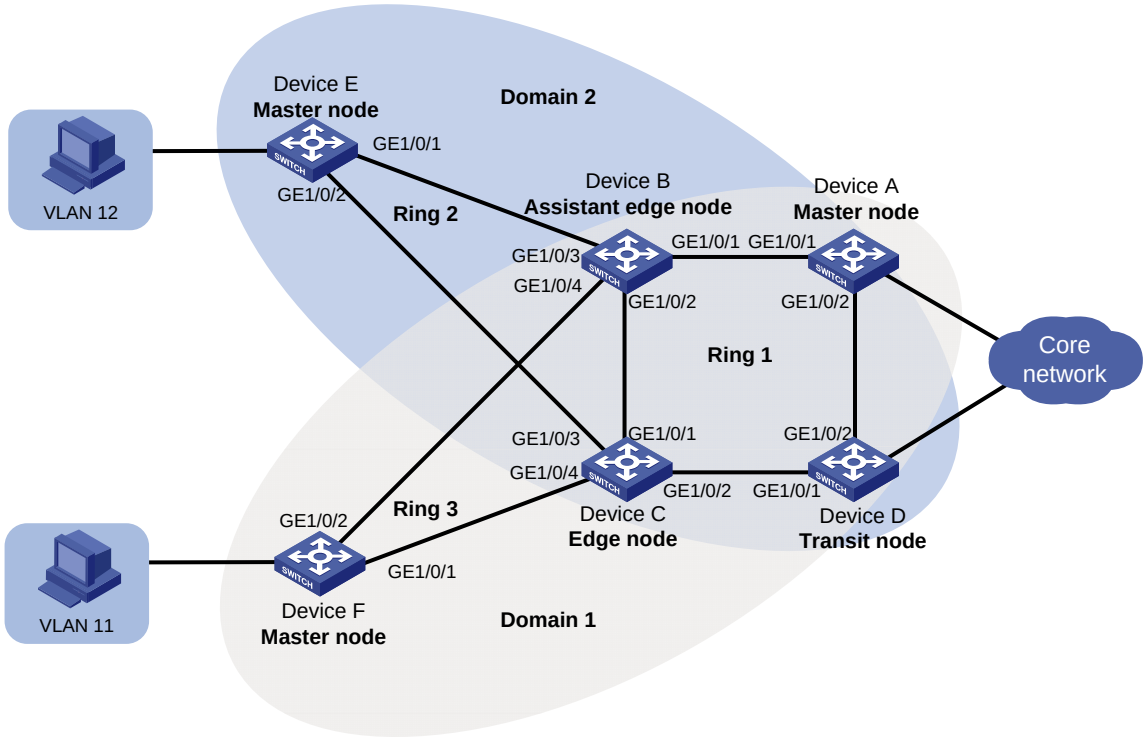
As shown in Figure 195:

- Two access-layer networks are connected to the distribution layer by using a ring topology.
- The distribution layer also adopts a ring topology.

Configure RRPP to meet the following requirements:

- High availability and convergence performance of the network.
- Traffic load sharing by VLAN. (Traffic of VLAN 12 is forwarded through domain 2, and traffic of VLAN 11 is forwarded through domain 1.)
- Reduced number of Edge-Hello packets.

Figure 195 Network diagram



Requirements analysis

To forward traffic of different VLANs through different domains (paths), configure multiple domains for a ring network. In this example:

- Configure Ring 1 and Ring 3 as the primary ring and subring for domain 1.
- Configure Ring 1 and Ring 2 as the primary ring and subring for domain 2.

The primary ring must feature high transmission capability for transparently transmitting traffic of the protected VLANs and control VLANs of the subrings. In this example,:

- Configure Ring 1 as the primary ring of both domain 1 and domain 2.
- Configure Ring 2 and Ring 3 as the subrings of domain 2 and domain 1, respectively.

For the primary ring, configure a device with high performance as the master node. For the subring, configure a device other than a common node as the master node. In this example:

- Configure Device A as the master node of Ring 1.
- Configure Device E and Device F as the master node of Ring 2 and Ring 3, respectively.

To reduce Edge-Hello traffic, adopt the RRPP ring group mechanism by assigning Ring 2 and Ring 3 with the same edge node and assistant-edge node to an RRPP ring group.

Configuration restrictions and guidelines

When you configure load balanced intersecting-ring, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.
- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before enabling the subrings on their separate master nodes. On an edge node or assistant-edge node, enable the primary ring of an RRPP domain before enabling the subrings of the RRPP domain.
- To assign an active ring to a ring group, do that on the assistant-edge node first and then on the edge node.
- Make sure the RRPP ring group on the edge node and the RRPP ring group on the assistant-edge node have the same configurations and activation status.

Configuration procedures

Configuring Device A

1. Create VLANs 11 and 12.

```
<DeviceA> system-view
[DeviceA] vlan 11 to 12
 Please wait... Done.
```

2. Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2, and activate the MST region configuration.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 11
[DeviceA-mst-region] instance 2 vlan 12
```

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

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.
```

   # Assign the port to VLAN 11 and VLAN 12

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 11 12
 Please wait... Done.
```

   # Configure VLAN 11 as the default VLAN.

```
[DeviceA-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 11 12
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 100
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

   # Create RRPP domain 2.

```
[DeviceA] rrpp domain 2
 Info: Create a new domain.
```

   # Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceA-rrpp-domain2] control-vlan 105
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port.

```
[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
```

Enable ring 1.

```
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

1. Create VLANs 11 and 12.

```
<DeviceB> system-view
[DeviceB] vlan 11 to 12
 Please wait... Done.
```

2. Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2, and activate the MST region configuration.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 11
[DeviceB-mst-region] instance 2 vlan 12
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.
```

Assign the port to VLAN 11 and VLAN 12.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 11 12
 Please wait... Done.
```

Configure VLAN 11 as the default VLAN.

```
[DeviceB-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 11 12
 Please wait... Done.
```

```
[DeviceB-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

   # Disable the spanning tree feature on GigabitEthernet 1/0/3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable
```

   # Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
 Please wait... Done.
```

   # Assign the port to VLAN 12.

```
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 12
 Please wait... Done.
```

   # Configure VLAN 12 as the default VLAN.

```
[DeviceB-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceB-GigabitEthernet1/0/3] quit
```

5. Configure GigabitEthernet 1/0/4:

   # Disable the spanning tree feature on GigabitEthernet 1/0/4.

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo stp enable
```

   # Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
 Please wait... Done.
```

   # Assign the port to VLAN 11.

```
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 11
 Please wait... Done.
```

   # Configure VLAN 11 as the default VLAN.

```
[DeviceB-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/4] quit
```

6. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 100
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device B as a transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 enable
```

Configure Device B as the assistant-edge node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/4 as the edge port.

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
```

Enable ring 3.

```
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceB] rrpp domain 2
 Info: Create a new domain.
```

Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceB-rrpp-domain2] control-vlan 105
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 enable
```

Configure Device B as the assistant-edge node of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
```

Enable ring 2.

```
[DeviceB-rrpp-domain2] ring 2 enable
[DeviceB-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C

1. Create VLANs 11 and 12.

```
<DeviceC> system-view
[DeviceC] vlan 11 to 12
 Please wait... Done.
```

2. Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2, and activate the MST region configuration.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 11
[DeviceC-mst-region] instance 2 vlan 12
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.
```

Assign the port to VLAN 11 and VLAN 12.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 11 12
 Please wait... Done.
```

Configure VLAN 11 as the default VLAN.

```
[DeviceC-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 11 12
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Disable the spanning tree feature on GigabitEthernet 1/0/3.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
 Please wait... Done.
```

Assign the port to VLAN 12.

```
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 12
 Please wait... Done.
```

Configure VLAN 12 as the default VLAN.

```
[DeviceC-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceC-GigabitEthernet1/0/3] quit
```

5. Configure GigabitEthernet 1/0/4:

Disable the spanning tree feature on GigabitEthernet 1/0/4.

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo stp enable
```

Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] undo port trunk permit vlan 1
 Please wait... Done.
```

Assign the port to VLAN 11.

```
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 11
 Please wait... Done.
```

Configure VLAN 11 as the default VLAN.

```
[DeviceC-GigabitEthernet1/0/4] port trunk pvid vlan 11
```

```
[DeviceC-GigabitEthernet1/0/4] quit
```

6. Configure RRPP:

Create RRPP domain 1.

```
[DeviceC] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
[DeviceC-rrpp-domain1] control-vlan 100
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device C as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 enable
```

Configure Device C as the edge node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/4 as the edge port.

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
```

Enable ring 3.

```
[DeviceC-rrpp-domain1] ring 3 enable
[DeviceC-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceC] rrpp domain 2
 Info: Create a new domain.
```

Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceC-rrpp-domain2] control-vlan 105
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device C as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 enable
```

Configure Device C as the edge node of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/3 as the edge port.

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet1/0/3
```

Enable ring 2.

```
[DeviceC-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceC] rrpp enable
```

Configuring Device D

1. Create VLANs 11 and 12.

```
<DeviceD> system-view
```

```
[DeviceD] vlan 11 to 12
 Please wait... Done.
```

2. Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2, and activate the MST region configuration.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 11
[DeviceD-mst-region] instance 2 vlan 12
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.
```

   # Assign the port to VLAN 11 and VLAN 12.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 11 12
 Please wait... Done.
```

   # Configure VLAN 11 as the default VLAN.

```
[DeviceD-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 11 12
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 100
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device D as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 enable
```

```
[DeviceD-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceD] rrpp domain 2
 Info: Create a new domain.
```

Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceD-rrpp-domain2] control-vlan 105
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device D as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Enable ring 1.

```
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceD] rrpp enable
```

Configuring Device E

1. Create VLAN 12.

```
<DeviceE> system-view
[DeviceE] vlan 12
 Please wait... Done.
[DeviceE-vlan12] quit
```

2. Map VLAN 12 to MSTI 2, and activate the MST region configuration.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 12
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.
```

Assign the port to VLAN 12.

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 12
 Please wait... Done.
```

Configure VLAN 12 as the default VLAN.

```
[DeviceE-GigabitEthernet1/0/1] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 12
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 2.

```
[DeviceE] rrpp domain 2
 Info: Create a new domain.
```

   # Configure VLAN 105 as the primary control VLAN.

```
[DeviceE-rrpp-domain2] control-vlan 105
```

   # Configure the VLANs mapped to MSTI 2 as the protected VLANs.

```
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

   # Configure Device E as the master mode of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

   # Enable ring 2.

```
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

   # Enable RRPP.

```
[DeviceE] rrpp enable
```

Configuring Device F

1. Create VLAN 11.

```
<DeviceF> system-view
[DeviceF] vlan 11
 Please wait... Done.
[DeviceF-vlan11] quit
```

2. Map VLAN 11 to MSTI 1, and activate the MST region configuration.

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 11
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and remove the port from VLAN 1.

```
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.
```

   # Assign the port to VLAN 11.

```
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 11
```

```
 Please wait... Done.
```

Configure VLAN 11 as the default VLAN.

```
[DeviceF-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 11
 Please wait... Done.
[DeviceF-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

Create RRPP domain 1.

```
[DeviceF] rrpp domain 1
 Info: Create a new domain.
```

Configure VLAN 100 as the primary control VLAN.

```
[DeviceF-rrpp-domain1] control-vlan 100
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs.

```
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device F as the master node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

Enable ring 3.

```
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceF] rrpp enable
```

Configuring RRPP ring groups on Device B and Device C

Create RRPP ring group 1 on Device B. Add subrings 2 and 3 to the RRPP ring group.

```
[DeviceB] rrpp ring-group 1
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3
```

Create RRPP ring group 1 on Device C. Add subrings 2 and 3 to the RRPP ring group.

```
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3
```

Verifying the configuration

1. Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "Example: Configuring single ring."

2. Display the brief RRPP information.

```
<DeviceA> display rrpp brief
Flags for Node Mode :
M -- Master , T -- Transit , E -- Edge , A -- Assistant-Edge

RRPP Protocol Status: Enable
Number of RRPP Domains: 2

Domain ID     : 1
Control VLAN  : Major 100    Sub 101
Protected VLAN: Reference Instance 1
Hello Timer   : 1  sec  Fail Timer : 3  sec
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
 Ring  Ring   Node  Primary/Common            Secondary/Edge            Enable
 ID    Level  Mode  Port                      Port                      Status
--------------------------------------------------------------------------------
 1     0      M     GE1/0/1                   GE1/0/2                   Yes

Domain ID     : 2
Control VLAN  : Major 105    Sub 106
Protected VLAN: Reference Instance 2
Hello Timer   : 1  sec  Fail Timer : 3  sec
Fast Detection Status: Disable
Fast Hello Timer: 200 ms     Fast Fail Timer: 600 ms
 Ring  Ring   Node  Primary/Common            Secondary/Edge            Enable
 ID    Level  Mode  Port                      Port                      Status
--------------------------------------------------------------------------------
 1     0      M     GE1/0/1                   GE1/0/2                   Yes
```

   The output shows the following:

   - The VLAN mapped to MSTI 1 is the protected VLAN of RRPP domain 1.
   - The VLAN mapped to MSTI 2 is the protected VLAN of RRPP domain 2.

   In this example, VLAN 11 is mapped to MSTI 1 and VLAN 12 is mapped to MSTI 2. Traffic from VLAN 11 and VLAN 12 are forwarded through RRPP domain 1 and RRPP domain 2, respectively.

3. Display the RRPP ring group configuration.

```
<DeviceB> display rrpp ring-group
Ring Group 1:
Domain 1 Ring 3
Domain 2 Ring 2
Domain 1 Ring 3 is the sending ring
```

   The output shows that RRPP group 1 takes effect, and only Ring 3 on Device B sends Edge-Hello packets.

Configuration files

- Device A:

```
#
```

```
vlan 11 to 12
#
stp region-configuration
 instance 1 vlan 11
 instance 2 vlan 12
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 105
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B:

```
#
vlan 11 to 12
#
stp region-configuration
 instance 1 vlan 11
 instance 2 vlan 12
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 12
 port trunk pvid vlan 12
 stp disable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 port trunk pvid vlan 11
 stp disable
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 3 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 3 enable
#
rrpp domain 2
 control-vlan 105
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp ring-group 1
 domain 2 ring 2
 domain 1 ring 3
#
rrpp enable
#
```

- Device C:

```
#
vlan 11 to 12
#
stp region-configuration
 instance 1 vlan 11
 instance 2 vlan 12
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 12
 port trunk pvid vlan 12
 stp disable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 port trunk pvid vlan 11
 stp disable
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 3 node-mode edge edge-port GigabitEthernet1/0/4
 ring 3 enable
#
rrpp domain 2
 control-vlan 105
 protected-vlan reference-instance 1
```

```
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp ring-group 1
 domain 2 ring 2
 domain 1 ring 3
#
rrpp enable
#
```

- Device D:

```
#
vlan 11 to 12
#
stp region-configuration
 instance 1 vlan 11
 instance 2 vlan 12
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 105
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
```

```
rrpp enable
#
```

- Device E:

```
#
vlan 12
#
stp region-configuration
 instance 2 vlan 12
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 12
 port trunk pvid vlan 12
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 12
 port trunk pvid vlan 12
 stp disable
#
rrpp domain 2
 control-vlan 105
 protected-vlan reference-instance 2
 ring 2 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 1
 ring 2 enable
#
rrpp enable
#
```

- Device F:

```
#
vlan 11
#
stp region-configuration
 instance 1 vlan 11
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 port trunk pvid vlan 11
 stp disable
#
```

```
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 port trunk pvid vlan 11
 stp disable
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 3 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 3 enable
#
rrpp enable
#
```

Example: Configuring fast detection

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

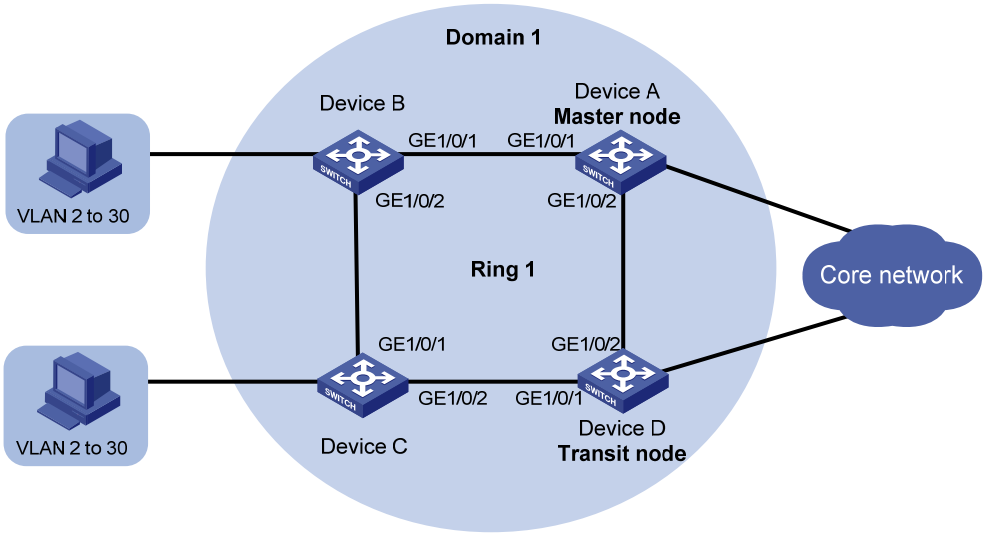
Network requirements

As shown in Figure 196:

- Multiple users are connected to the distribution-layer network that adopts an RRPP ring topology.
- Device B and Device C do not support RRPP.

In practice, some devices on an RRPP ring might not support RRPP. RRPP can detect link failures between these devices only through the timeout mechanism. This results in long-time traffic interruption and failure to implement millisecond-level convergence. To ensure high reliability and convergence performance of the network, enable fast detection on the RRPP ring.

Figure 196 Network diagram



Requirements analysis

The master node initiates the polling mechanism and determines the operations to be performed after a change in topology. Therefore, you must configure a device with high performance as the master node. In this example, configure Device A as the master node.

To transparently transmit RRPPDUs on a device that is not configured with RRPP, make sure only the two ports connecting the device to the RRPP ring permit packets from the control VLANs. Otherwise, the packets from other VLANs might enter the control VLANs in transparent transmission mode and strike the RRPP ring.

Configuration restrictions and guidelines

When you configure fast detection, follow these restrictions and guidelines:

- The HP 7500 Switch Series supports RRPP fast detection only after SD or EB cards are mounted in it.
- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.

Configuration procedures

Configuring Device A

1. Create VLANs 2 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device A as the master node of the primary ring Ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 enable
```

   # Enable fast detection. Set the Fast-Fail timer and Fast-Hello timer to 300 milliseconds and 100 milliseconds, respectively.

```
[DeviceA-rrpp-domain1] fast-detection enable
[DeviceA-rrpp-domain1] quit
```

   # Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

1. Create VLANs 2 through 30, VLAN 4092, and VLAN 4093.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 30
 Please wait... Done.
```

```
[DeviceB] vlan 4092 to 4093
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30, 4092, and 4093.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30 4092 4093
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30 4092 4093
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

1. Create VLANs 2 through 30, VLAN 4092, and VLAN 4093.

```
<DeviceC> system-view
[DeviceC] vlan 2 to 30
 Please wait... Done.
[DeviceC] vlan 4092 to 4093
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30, 4092, and 4093.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30 4092 4093
 Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30 4092 4093
 Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Create VLANs 2 through 30.

```
<DeviceD] system-view
[DeviceD] vlan 2 to 30
```

```
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 2 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure RRPP:

   # Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
 Info: Create a new domain.
```

   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

   # Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

   # Configure Device D as a transit node of the primary ring Ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

   # Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

   # Enable RRPP.

```
[DeviceD] rrpp enable
```

Verifying the configuration

Use the **display rrpp verbose** command to view RRPP configuration and operational information on Device A and Device D. For more information, see "Example: Configuring single ring."

Configuration files

- Device A:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 fast-detection enable
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B:

```
#
vlan 2 to 30
#
vlan 4092 to 4093
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30 4092 to 4093
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30 4092 to 4093
 stp disable
#
```

- Device C:

```
#
```

```
vlan 2 to 30
#
vlan 4092 to 4093
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30 4092 to 4093
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30 4092 to 4093
 stp disable
#
```

- Device D:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

Example: Configuring RRPP and Smart Link

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

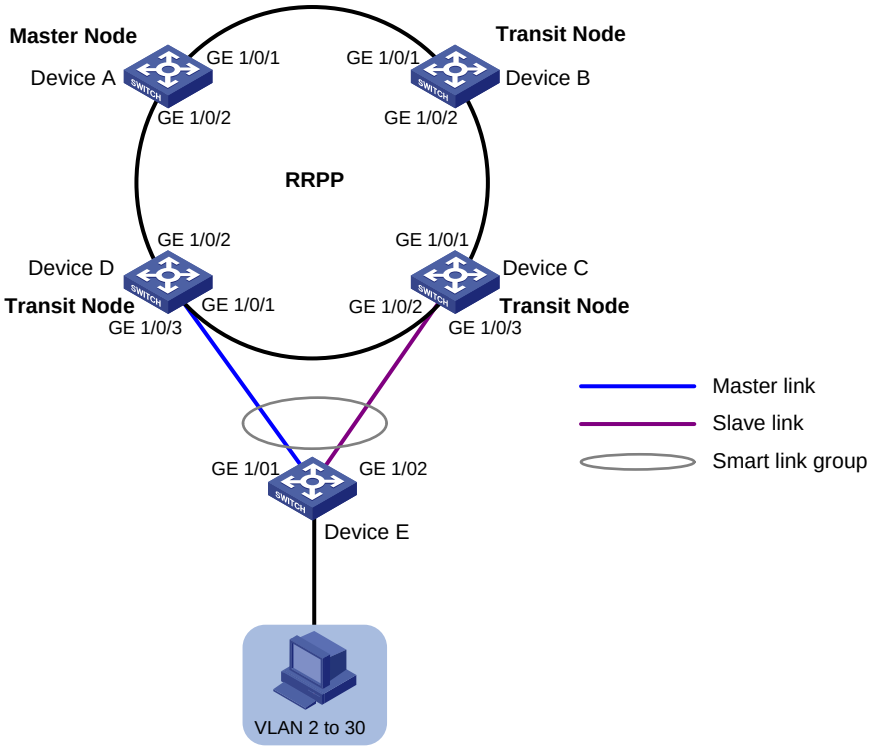
Network requirements

As shown in Figure 197:

- Device A through Device D support RRPP.
- Device E is a Smart Link device dually uplinked to the distribution layer that adopts a ring topology.

Because Device E at the access layer does not support RRPP, you can use RRPP with Smart Link as a substitution of the RRPP intersecting ring configuration. Configure an RRPP single ring at the distribution layer, and configure Smart Link on the access-layer device. This method ensures high reliability and convergence performance of both the access layer and the distribution layer.

Figure 197 Network diagram



Requirements analysis

For information about Requirements analysis for configuring a single ring, see "Example: Configuring single ring."

Configuration restrictions and guidelines

When you configure RRPP and Smart Link, follow these restrictions and guidelines:

- For information about configuration restrictions and guidelines for configuring a single ring, see "Example: Configuring single ring."
- To prevent loops, shut down a port and then disable the spanning tree feature before configuring it as a smart link group member. You can bring up the port only after completing the smart link group configuration.
- When you configure Device C and Device D, disable the spanning tree feature on the ports that are connected to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in forwarding state when a topology change occurs.
- Make sure the receive control VLAN on Device C and Device D is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, Device C and Device D might not receive and process flush messages correctly.

Configuration procedures

Configuring RRPP single ring

Configure the RRPP single ring on Device A through Device D. For more information, see "Example: Configuring single ring."

Configuring Device E

1. Create VLANs 2 through 30.

```
<DeviceE> system-view
[DeviceE] vlan 2 to 30
 Please wait... Done.
```

2. Map the VLANs to MSTI 1, and activate the MST region configuration.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 2 to 30
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

3. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Shut down GigabitEthernet 1/0/1.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] shutdown
```

   # Disable the spanning tree feature on the port.

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

   # Configure the port as a trunk port and assign it to VLANs 2 through 30.

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
```

```
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] shutdown
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] quit
```

4. Configure smart link group 1:

Create smart link group 1, and configure all VLANs mapped to MSTI 1 as the protected VLANs.

```
[DeviceE] smart-link group 1
[DeviceE-smlk-group1] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

```
[DeviceE-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceE-smlk-group1] port gigabitethernet 1/0/2 slave
```

Enable flush message sending in smart link group 1. Configure VLAN 10 as the transmit control VLAN.

```
[DeviceE-smlk-group1] flush enable control-vlan 10
[DeviceE-smlk-group1] quit
```

5. Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] quit
```

Configuring Device C

Disable the spanning tree feature on GigabitEthernet 1/0/3.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

Configure the port as a trunk port.

```
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLANs 2 through 30.

```
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceC-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceC-GigabitEthernet1/0/3] quit
```

Configuring Device D

Disable the spanning tree feature on GigabitEthernet 1/0/3.

```
[DeviceD] interface gigabitethernet 1/0/3
```

```
[DeviceD-GigabitEthernet1/0/3] undo stp enable
```

Configure the port as a trunk port.

```
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLANs 2 through 30.

```
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceD-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceD-GigabitEthernet1/0/3] quit
```

Verifying the configuration

1. Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "Example: Configuring single ring."
2. Display the smart link group information.

   # Display the information about smart link group 1 on Device C.

```
[DeviceE] display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: NONE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   5           16:37:20 2013/02/21

 GigabitEthernet1/0/2      SLAVE   STANDBY  1           17:45:20 2013/02/21
```

   # Display the flush messages received on Device D.

```
[DeviceD] display smart-link flush
 Received flush packets                          : 5
 Receiving interface of the last flush packet    : GigabitEthernet1/0/3
 Receiving time of the last flush packet         : 16:25:21 2013/02/21
 Device ID of the last flush packet              : 000f-e23d-5af0
 Control VLAN of the last flush packet           : 10
```

Configuration files

For information about the RRPP single ring configuration files on Device A through Device D, see "Example: Configuring single ring."

- Device C:

```
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
```

```
 smart-link flush enable control-vlan 10
#
```

- Device D:

```
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 smart-link flush enable control-vlan 10
#
```

- Device E:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
smart-link group 1
 protected-vlan reference-instance 1
 flush enable control-vlan 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 port smart-link group 1 master
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 port smart-link group 1 slave
#
```

Sampler configuration examples

This chapter provides sampler configuration examples.

Example: Configuring a sampler

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

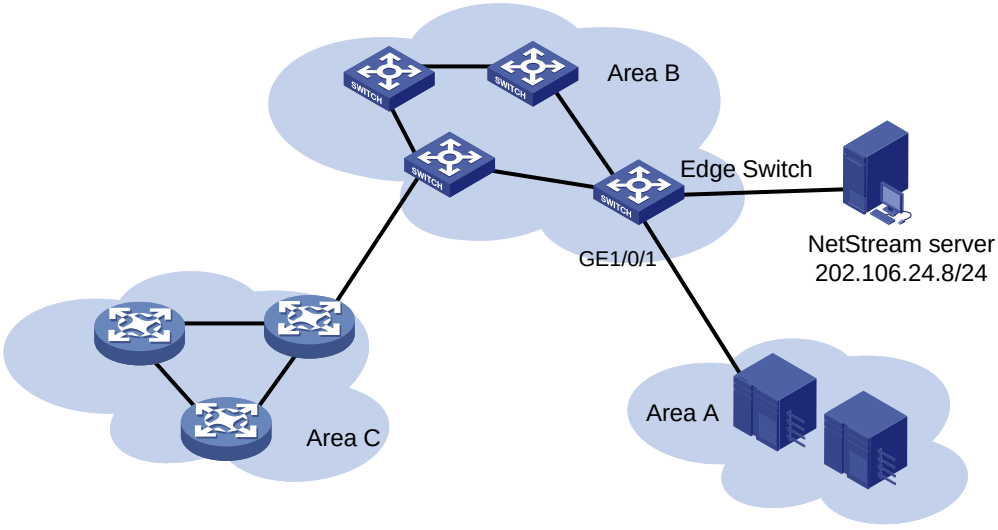
Network requirements

As shown in Figure 198, Area A is the data center area, and Area B and Area C are the user areas. NetStream is configured on the edge switch to monitor the traffic leaving the data center area.

Configure a sampler on the edge switch to meet the following requirements:

- Limit the volume of traffic to be analyzed.
- Minimize the impact of sampling on the forwarding performance of the device.

Figure 198 Network diagram



Configuration restrictions and guidelines

HP 7500 switches support only the fixed sampling mode.

Configuration procedures

Create sampler **sam256** in fixed sampling mode. Set the rate to 8, which means that one packet out of 256 (2 to the 8th power) packets is selected.

```
<EdgeSwitch> system-view
[EdgeSwitch] sampler sam256 mode fixed packet-interval 8
```

Enable NetStream sampling in the inbound direction of GigabitEthernet 1/0/1 by referencing sampler **sam256**.

```
[EdgeSwitch] interface GigabitEthernet 1/0/1
[EdgeSwitch-GigabitEthernet1/0/1] ip netstream inbound
[EdgeSwitch-GigabitEthernet1/0/1] ip netstream sampler sam256 inbound
[EdgeSwitch-GigabitEthernet1/0/1] quit
```

Configure the destination address as 202.106.24.8 and the destination UDP port number as 5000 for the NetStream data export.

```
[EdgeSwitch] ip netstream export host 202.106.24.8 5000
```

Verifying the configuration

Execute the **display sampler** command on the edge switch to view the configuration information about sampler **sam256**.

```
[EdgeSwitch] display sampler
 Sampler name: sam256
  Index: 1,  Mode: Fixed,  Packet-interval: 8
```

Configuration files

```
#
 sampler sam256 mode fixed packet-interval 8
#
interface GigabitEthernet1/0/1
 ip netstream inbound
 ip netstream sampler sam256 inbound
#
 ip netstream export host 202.106.24.8 5000
```

sFlow configuration examples

This chapter provides sFlow configuration examples.

Example: Configuring sFlow

Applicable product matrix

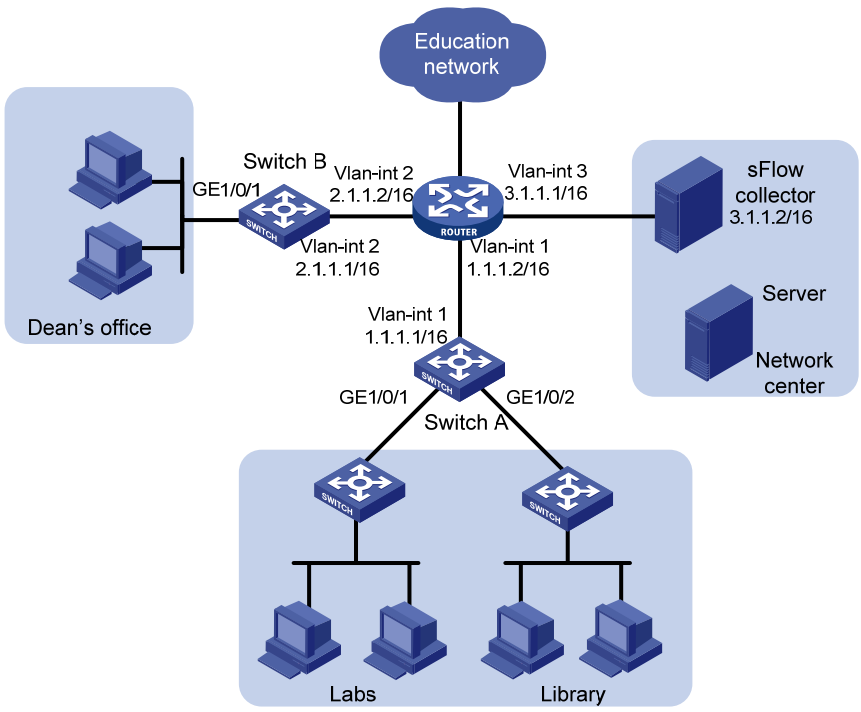
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 199:

- Configure flow sampling and counter sampling on the following ports to monitor their traffic:
  - GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A.
  - GigabitEthernet 1/0/1 of Switch B.
- Configure Switch A and Switch B to send sampled information in sFlow packets to the sFlow collector that uses the port number 5000.

Figure 199 Network diagram



Configuration restrictions and guidelines

When you configure sFlow, follow these restrictions and guidelines:

- Set a low sampling rate on the ports with many hosts connected to Switch A. Set a high sampling rate on the port with a few hosts connected to Switch B.
- Set a long counter sampling interval on the ports with many hosts connected to Switch A. Set a short counter sampling interval on the port with a few hosts connected to Switch B.
- Make sure the devices can reach each other before the sFlow configuration.
- Configure the sFlow agents with the same sFlow collector IP address as the remote sFlow collector. Otherwise, the remote sFlow collector cannot receive sFlow packets.

Configuration procedures

Configuring Switch A

Configure the IP address of the sFlow agent.

```
<SwitchA> system-view
[SwitchA] sflow agent ip 1.1.1.1
```

Configure the sFlow collector ID as **1**, IP address as **3.1.1.2**, and port number as **5000**.

```
[SwitchA] sflow collector 1 ip 3.1.1.2 port 5000
```

Set the counter sampling interval to **120** seconds. Specify the sFlow collector ID as **1**.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] sflow counter interval 120
[SwitchA-GigabitEthernet1/0/1] sflow counter collector 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] sflow counter interval 120
[SwitchA-GigabitEthernet1/0/2] sflow counter collector 1
[SwitchA-GigabitEthernet1/0/2] quit
```

Set the flow sampling rate to **100000** (one packet is sampled from every 100000 packets). Specify the sFlow collector ID as **1**.

```
[SwitchA-GigabitEthernet1/0/1] sflow sampling-rate 100000
[SwitchA-GigabitEthernet1/0/1] sflow flow collector 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] sflow sampling-rate 100000
[SwitchA-GigabitEthernet1/0/2] sflow flow collector 1
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B

Configure the IP address for the sFlow agent.

```
<SwitchB> system-view
[SwitchB] sflow agent ip 2.1.1.1
```

Configure the sFlow collector ID as **1**, IP address as **3.1.1.2**, and port number as **5000**.

```
[SwitchB] sflow collector 2 ip 3.1.1.2 port 5000
```

Set the counter sampling interval to **30** seconds. Specify the sFlow collector ID as **1**.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] sflow counter interval 30
[SwitchB-GigabitEthernet1/0/1] sflow counter collector 1
```

Set the flow sampling rate to **20000** (one packet is sampled from every 20000 packets). Specify the sFlow collector ID as **1**.

```
[SwitchB-GigabitEthernet1/0/1] sflow sampling-rate 20000
[SwitchB-GigabitEthernet1/0/1] sflow flow collector 1
[SwitchB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the sFlow configuration and operation information. This example uses Switch A.

```
[SwitchA] display sflow
sFlow Version: 5
sFlow Global Information:
Agent        IP:1.1.1.1(CLI)
Source  Address:
Collector Information:
ID   IP                      Port  Aging      Size   VPN-instance Description
1    3.1.1.2                 5000  N/A        1400                CLI Collector
2                            6343  0          1400
3                            6343  0          1400
4                            6343  0          1400
5                            6343  0          1400
6                            6343  0          1400
7                            6343  0          1400
8                            6343  0          1400
9                            6343  0          1400
10                           6343  0          1400
sFlow Port Information:
Interface       CID Interval(s) FID MaxHLen Rate     Mode      Status
GE1/0/1         1   120          1   128     100000   Random    Active
GE1/0/2         1   120          1   128     100000   Random    Active
```

Configuration files

- Switch A:

```
#
 sflow agent ip 1.1.1.1
 sflow collector 1 ip 3.1.1.2 port 5000
#
interface GigabitEthernet1/0/1
 sflow sampling-rate 100000
 sflow flow collector 1
 sflow counter interval 120
 sflow counter collector 1
#
```

```
interface GigabitEthernet1/0/2
 sflow sampling-rate 100000
 sflow flow collector 1
 sflow counter interval 120
 sflow counter collector 1
#
```

- Switch B:

```
#
 sflow agent ip 2.1.1.1
 sflow collector 1 ip 3.1.1.2 port 5000
#
interface GigabitEthernet1/0/1
 sflow sampling-rate 20000
 sflow flow collector 1
 sflow counter interval 30
 sflow counter collector 1
#
```

Smart Link and CFD collaboration configuration examples

This chapter provides Smart Link and Connectivity Fault Detection (CFD) collaboration configuration examples.

Smart Link supports the Continuity Check (CC) function of CFD to implement link detection. When a fault is detected or cleared, CFD informs Smart Link to switch over the links.

General configuration restrictions and guidelines

When you configure Smart Link and CFD collaboration, follow these restrictions and guidelines:

- Disable the spanning tree feature and RRPP on the ports that you want to add to a smart link group.
- Make sure the ports are not member ports of any aggregation group or service loopback group.

Example: Single smart link group and CFD collaboration configuration example

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

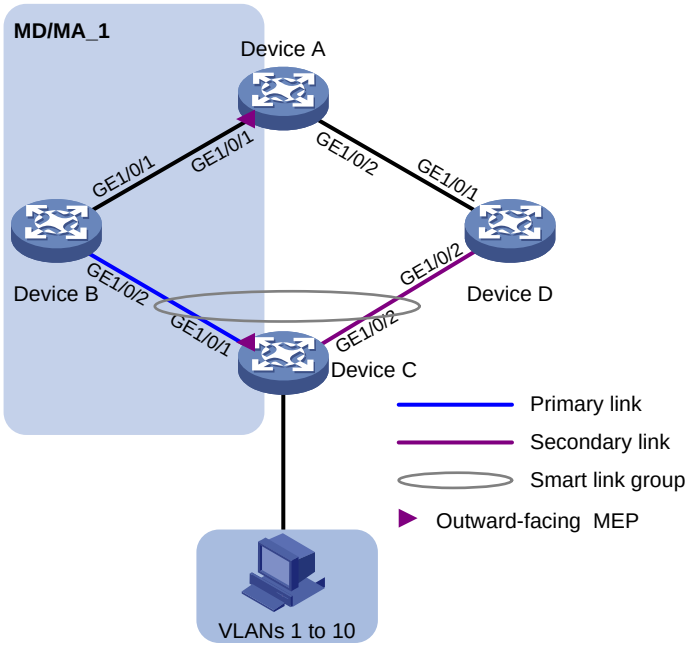
Network requirements

As shown in Figure 200, traffic of VLANs 1 through 10 on Device C is dually uplinked to Device A by Device B and Device D.

Configure Smart Link and CFD collaboration on Device C, and configure CFD on Device C and Device A to meet the following requirements:

- User traffic is forwarded through the primary port of the smart link group on Device C.
- When the link between the primary port and Device A fails, the secondary port of the smart link group immediately transits to forwarding state.
- When the link between the primary port and Device A recovers, the primary port of the smart link group transits to forwarding state.

Figure 200 Network diagram



Requirements analysis

In this example, to enable Device C to prefer Device B to forward user traffic to Device A, configure GigabitEthernet 1/0/1 as the primary port of the smart link group on Device C.

To make sure the primary port of the smart link group immediately transits to forwarding state when the primary link recovers, configure role preemption for the smart link group.

Configuration restrictions and guidelines

When you configure single smart link group and CFD collaboration, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in the forwarding state when a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- Make sure the receive control VLAN is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.
- Make sure the control VLAN of the smart link group matches the detection VLAN of the CC function of CFD.

Configuration procedures

Configuring Device C

1. Configure VLAN and MST region settings:

   # Create VLAN 1 through VLAN 10.

   ```
   <DeviceC> system-view
   [DeviceC] vlan 1 to 10
    Please wait... Done.
   ```

   Map these VLANs to MSTI 0.

   ```
   [DeviceC] stp region-configuration
   [DeviceC-mst-region] instance 0 vlan 1 to 10
   ```

   # Activate MST region configuration.

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Shut down GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/1
   [DeviceC-GigabitEthernet1/0/1] shutdown
   ```

   # Disable the spanning tree feature on the port.

   ```
   [DeviceC-GigabitEthernet1/0/1] undo stp enable
   ```

   # Configure the port as a trunk port, and assign the port to VLAN 1 through VLAN 10.

   ```
   [DeviceC-GigabitEthernet1/0/1] port link-type trunk
   [DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/2
   [DeviceC-GigabitEthernet1/0/1] shutdown
   [DeviceC-GigabitEthernet1/0/2] undo stp enable
   [DeviceC-GigabitEthernet1/0/2] port link-type trunk
   [DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/2] quit
   ```

3. Configure smart link group 1:

   # Create smart link group 1.

   ```
   [DeviceC] smart-link group 1
   ```

   # Configure all VLANs mapped to MSTI 0 as the protected VLANs.

   ```
   [DeviceC-smlk-group1] protected-vlan reference-instance 0
   ```

   # Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

   ```
   [DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
   [DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
   ```

   # Enable role preemption in smart link group 1.

   ```
   [DeviceC-smlk-group1] preemption mode role
   ```

Enable flush update for smart link group 1, and specify VLAN 10 as the control VLAN.

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

4. Configure CFD:

Enable CFD.

```
<DeviceC> system-view
[DeviceC] cfd enable
```

Create service instance 1 in which the MA serves VLAN 10.

```
[DeviceC] cfd md MD level 5
[DeviceC] cfd ma MA_1 md MD vlan 10
[DeviceC] cfd service-instance 1 md MD ma MA_1
```

Configure MEPs.

```
[DeviceC] cfd meplist 1001 1002 service-instance 1
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceC-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
```

Enable the sending of CCM frames for MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Configuring Device B

1. Create VLAN 1 through VLAN 10.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 10
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 10.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Create VLAN 1 through VLAN 10.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 10
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 10.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 10.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceD-GigabitEthernet1/0/2] quit
```

Configuring Device A

1. Create VLAN 1 through VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 10
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 10.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceA-GigabitEthernet1/0/2] quit
```

3. Configure CFD:

Enable CFD.

```
<DeviceA> system-view
[DeviceA] cfd enable
```

Create service instance 1 in which the MA serves VLAN 10.

```
[DeviceA] cfd md MD level 5
[DeviceA] cfd ma MA_1 md MD vlan 10
[DeviceA] cfd service-instance 1 md MD ma MA_1
```

Configure MEPs.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1002 enable
```

Enable the sending of CCM frames for MEP 1002 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring the collaboration between Smart Link and the CC function of CFD

Configure the collaboration between Smart Link and the CC function of CFD on Device C.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
[DeviceC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

After you shut down GigabitEthernet 1/0/1 on Device B, use the **display smart-link group** command to display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 0023-895f-954f
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 0
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
```

```
GigabitEthernet1/0/1       MASTER  DOWN     0           NA
GigabitEthernet1/0/2       SLAVE   ACTIVE   1           14:32:56 2012/12/11
```

The output shows the following:

- Primary port GigabitEthernet 1/0/1 of smart link group 1 fails.
- Secondary port GigabitEthernet 1/0/2 is in forwarding state.
- A link switchover occurs.

Configuration files

- Device A:

```
#
 cfd enable
 cfd md MD level 5
 cfd ma MA_1 md MD vlan 10
 cfd service-instance 1 md MD ma MA_1
 cfd meplist 1001 to 1002 service-instance 1
#
vlan 1
#
vlan 2 to 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 10
 smart-link flush enable control-vlan 10
 cfd mep 1002 service-instance 1 outbound
 cfd mep service-instance 1 mep 1002 enable
 cfd cc service-instance 1 mep 1002 enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 10
 smart-link flush enable control-vlan 10
#
```

- Device B:

```
#
vlan 1
#
vlan 2 to 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 10
 smart-link flush enable control-vlan 10
#
interface GigabitEthernet1/0/2
```

```
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 smart-link flush enable control-vlan 10
#
```

- Device C:

```
#
 cfd enable
 cfd md MD level 5
 cfd ma MA_1 md MD vlan 10
 cfd service-instance 1 md MD ma MA_1
 cfd meplist 1001 to 1002 service-instance 1
#
vlan 1
#
vlan 2 to 10
#
stp region-configuration
 instance 0 vlan 1 to 10
 active region-configuration
#
smart-link group 1
 preemption mode role
 protected-vlan reference-instance 0
 flush enable control-vlan 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 port smart-link group 1 master
 port smart-link group 1 track cfd cc
 cfd mep 1001 service-instance 1 outbound
 cfd mep service-instance 1 mep 1001 enable
 cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 port smart-link group 1 slave
#
```

- Device D:

```
#
vlan 1
#
vlan 2 to 10
#
```

```
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 10
 smart-link flush enable control-vlan 10
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 smart-link flush enable control-vlan 10
#
```

Example: Multiple smart link groups and CFD collaboration configuration example

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

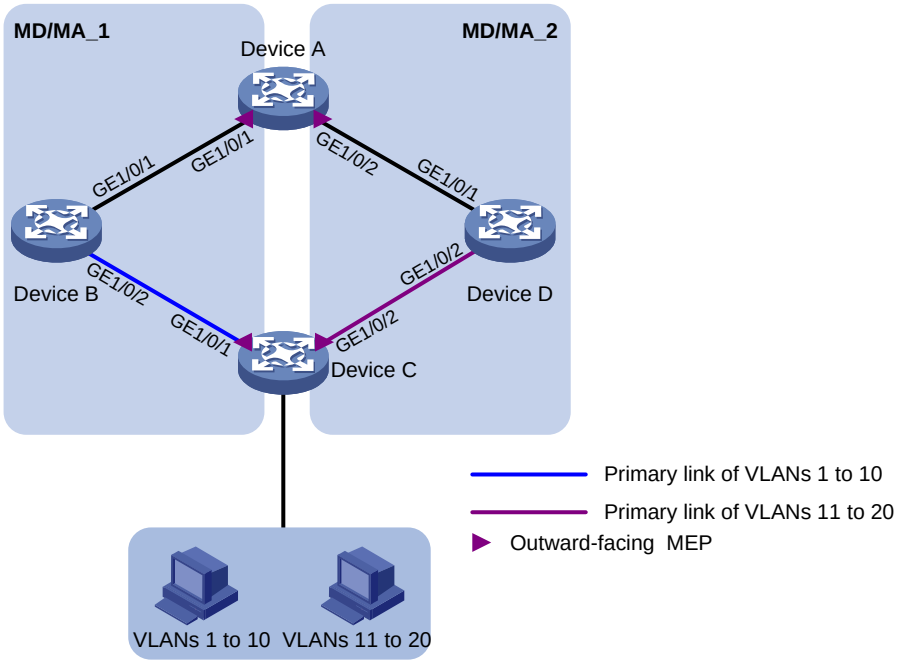
Network requirements

As shown in Figure 201, traffic of VLANs 1 through 20 on Device C is dually uplinked to Device A by Device B and Device D.

Configure multiple smart link groups and CFD collaboration on Device C, and configure CFD on Device C and Device A to meet the following requirements:

- Traffic of VLANs 1 through 10 is uplinked to Device A by Device B. Traffic of VLANs 11 through 20 is uplinked to Device A by Device D.
- When the links between primary ports of the smart link groups and Device A fail, the secondary ports immediately transit to forwarding state.
- When the links between the primary ports and Device A recover, the primary ports of the smart link groups transit to forwarding state. Traffic load sharing is implemented.

Figure 201 Network diagram



Requirements analysis

In this example, to enable Device C to forward traffic of VLANs 1 through 10 through Device B and traffic of VLANs 11 through 20 through Device D, do the following:

Configure GigabitEthernet 1/0/1 as the primary port for smart link group 1.

Configure GigabitEthernet 1/0/2 as the primary port for smart link group 2 on Device C.

To make sure the primary port of the smart link group immediately transits to forwarding state when the primary link recovers, configure role preemption for the smart link group.

Configuration restrictions and guidelines

When you configure multiple smart link groups and CFD collaboration, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in the forwarding state when a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- Make sure the receive control VLAN is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.
- Make sure the control VLAN of the smart link group matches the detection VLAN of the CC function of CFD.

Configuration procedures

Configuring Device C

1. Configure VLAN and MST region settings:

   # Create VLAN 1 through VLAN 20.

   ```
   <DeviceC> system-view
   [DeviceC] vlan 1 to 20
    Please wait... Done.
   ```

   # Map VLANs 1 through 10 to MSTI 0, and VLANs 11 through 20 to MSTI 1.

   ```
   [DeviceC] stp region-configuration
   [DeviceC-mst-region] instance 0 vlan 1 to 10
   [DeviceC-mst-region] instance 1 vlan 11 to 20
   ```

   # Activate MST region configuration.

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Shut down GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/1
   [DeviceC-GigabitEthernet1/0/1] shutdown
   ```

   # Disable the spanning tree feature on the port.

   ```
   [DeviceC-GigabitEthernet1/0/1] undo stp enable
   ```

   # Configure the port as a trunk port, and assign the port to VLAN 1 through VLAN 20.

   ```
   [DeviceC-GigabitEthernet1/0/1] port link-type trunk
   [DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/2
   [DeviceC-GigabitEthernet1/0/2] shutdown
   [DeviceC-GigabitEthernet1/0/2] undo stp enable
   [DeviceC-GigabitEthernet1/0/2] port link-type trunk
   [DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/2] quit
   ```

3. Configure smart link group 1:

   # Create smart link group 1.

   ```
   [DeviceC] smart-link group 1
   ```

   # Configure all VLANs mapped to MSTI 0 as the protected VLANs for smart link group 1.

   ```
   [DeviceC-smlk-group1] protected-vlan reference-instance 0
   ```

   # Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

   ```
   [DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
   [DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
   ```

   # Enable role preemption in smart link group 1.

```
[DeviceC-smlk-group1] preemption mode role
```

Enable flush update for smart link group 1, and specify VLAN 10 as the control VLAN.

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

4. Configure smart link group 2:

Create smart link group 2.

```
[DeviceC] smart-link group 2
```

Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 2.

```
[DeviceC-smlk-group2] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port for smart link group 2.

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
```

Enable role preemption in smart link group 2.

```
[DeviceC-smlk-group2] preemption mode role
```

Enable flush update for smart link group 2, and specify VLAN 20 as the control VLAN.

```
[DeviceC-smlk-group2] flush enable control-vlan 20
[DeviceC-smlk-group2] quit
```

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

5. Configure CFD:

Enable CFD.

```
<DeviceC> system-view
[DeviceC] cfd enable
```

Create service instance 1, in which the MA serves VLAN 10.

```
[DeviceC] cfd md MD level 5
[DeviceC] cfd ma MA_1 md MD vlan 10
[DeviceC] cfd service-instance 1 md MD ma MA_1
```

Create service instance 2, in which the MA serves VLAN 20.

```
[DeviceC] cfd ma MA_2 md MD vlan 20
[DeviceC] cfd service-instance 2 md MD ma MA_2
```

Configure MEPs.

```
[DeviceC] cfd meplist 1001 1002 service-instance 1
[DeviceC] cfd meplist 2001 2002 service-instance 2
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceC-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceC-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2001 enable
```

Enable the sending of CCM frames for MEPs.

```
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device B

1. Create VLAN 1 through VLAN 20.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Create VLAN 1 through VLAN 20.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

   # Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
```

   # Disable the spanning tree feature.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

   # Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/2] quit
```

Configuring Device A

1. Create VLAN 1 through VLAN 20.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLAN 1 through VLAN 20.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

   # Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

3. Configure CFD:

   # Enable CFD.

```
<DeviceA> system-view
[DeviceA] cfd enable
```

   # Create service instance 1, in which the MA serves VLAN 10.

```
[DeviceA] cfd md MD level 5
[DeviceA] cfd ma MA_1 md MD vlan 10
[DeviceA] cfd service-instance 1 md MD ma MA_1
```

Create service instance 2, in which the MA serves VLAN 20.

```
[DeviceA] cfd ma MA_2 md MD vlan 20
[DeviceA] cfd service-instance 2 md MD ma MA_2
```

Configure MEPs.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2002 enable
```

Enable the sending of CCM frames for MEPs.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring the collaboration between Smart Link and the CC function of CFD

Configure the collaboration between Smart Link and the CC function of CFD on Device C.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track cfd cc
```

Verifying the configuration

After you shut down GigabitEthernet 1/0/1 on Device B, use the **display smart-link group** command to display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 0023-895f-954f
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 0
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  DOWN     0           NA
 GigabitEthernet1/0/2      SLAVE   ACTIVE   1           14:32:56 2012/12/11

 Smart link group 2 information:
 Device ID: 0023-895f-954f
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 20
```

```
Protected VLAN: Reference Instance 1
Member                    Role    State    Flush-count Last-flush-time
--------------------------------------------------------------------------------
GigabitEthernet1/0/2      MASTER  ACTIVE   0           NA
GigabitEthernet1/0/1      SLAVE   DOWN     0           NA
```

The output shows the following:

- Primary port GigabitEthernet 1/0/1 of smart link group 1 fails.
- Secondary port GigabitEthernet 1/0/2 is in forwarding state.
- A link switchover occurs.

Configuration files

- Device A:

```
#
 cfd enable
 cfd md MD level 5
 cfd ma MA_1 md MD vlan 10
 cfd service-instance 1 md MD ma MA_1
 cfd meplist 1001 to 1002 service-instance 1
 cfd ma MA_2 md MD vlan 20
 cfd service-instance 2 md MD ma MA_2
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
 cfd mep 1002 service-instance 1 outbound
 cfd mep service-instance 1 mep 1002 enable
 cfd cc service-instance 1 mep 1002 enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
 cfd mep 2002 service-instance 2 outbound
 cfd mep service-instance 2 mep 2002 enable
 cfd cc service-instance 2 mep 2002 enable
#
```

- Device B:

```
#
vlan 1
#
```

```
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10 20
#
```

- Device C:

```
#
 cfd enable
 cfd md MD level 5
 cfd ma MA_1 md MD vlan 10
 cfd service-instance 1 md MD ma MA_1
 cfd meplist 1001 to 1002 service-instance 1
 cfd ma MA_2 md MD vlan 20
 cfd service-instance 2 md MD ma MA_2
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 1
#
vlan 2 to 20
#
stp region-configuration
 instance 0 vlan 1 to 10
 instance 1 vlan 11 to 20
 active region-configuration
#
smart-link group 1
 preemption mode role
 protected-vlan reference-instance 0
 flush enable control-vlan 10
smart-link group 2
 preemption mode role
 protected-vlan reference-instance 1
 flush enable control-vlan 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 master
 port smart-link group 1 track cfd cc
```

```
 port smart-link group 2 slave
 cfd mep 1001 service-instance 1 outbound
 cfd mep service-instance 1 mep 1001 enable
 cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
 port smart-link group 2 master
 port smart-link group 2 track cfd cc
 cfd mep 2001 service-instance 2 outbound
 cfd mep service-instance 2 mep 2001 enable
 cfd cc service-instance 2 mep 2001 enable
#
```

- Device D:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10 20
#
```

Smart Link configuration examples

This chapter provides Smart Link configuration examples.

Smart Link provides link redundancy as well as fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails.

General configuration restrictions and guidelines

Disable the spanning tree feature and RRPP on the ports that you want to add to a smart link group, and make sure the ports are not member ports of any aggregation group or service loopback group.

Example: Configuring single smart link group

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

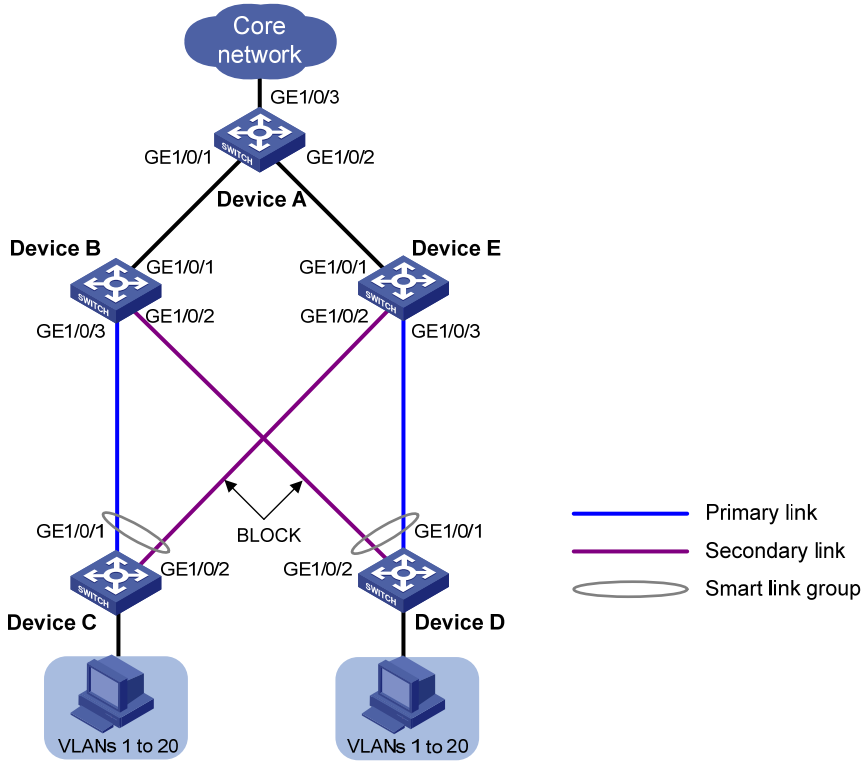
As shown in Figure 202:

- Device C and Device D are each connected to a user network consisting of VLANs 1 through 20.
- Device C and Device D are dually uplinked to Device A through Device B and Device E.

Configure Smart Link on Device C and Device D to meet the following requirements:

- Enable Device C to prefer Device B, and Device D to prefer Device E to forward user traffic to Device A.
- When one forwarding link fails, user traffic is immediately switched to another link to implement dual uplink backup.

Figure 202 Network diagram



Requirements analysis

In this example, to enable Device C to prefer Device B, and Device D to prefer Device E to forward user traffic to Device A, configure GigabitEthernet 1/0/1 as the primary port of the smart link group on Device C and Device D.

Configuration restrictions and guidelines

When you configure single smart link group, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in the forwarding state when a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- Make sure the receive control VLAN configured on the associated device is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.

Configuration procedures

Configuring Device C

1. Configure VLAN and MST region settings:

   # Create VLAN 1 through VLAN 20.

   ```
   <DeviceC> system-view
   [DeviceC] vlan 1 to 20
    Please wait... Done.
   ```

   # Map these VLANs to MSTI 1.

   ```
   [DeviceC] stp region-configuration
   [DeviceC-mst-region] instance 1 vlan 1 to 20
   ```

   # Activate MST region configuration.

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Shut down GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/1
   [DeviceC-GigabitEthernet1/0/1] shutdown
   ```

   # Disable the spanning tree feature on the port.

   ```
   [DeviceC-GigabitEthernet1/0/1] undo stp enable
   ```

   # Configure the port as a trunk port, and assign the port to VLAN 1 through VLAN 20.

   ```
   [DeviceC-GigabitEthernet1/0/1] port link-type trunk
   [DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/2
   [DeviceC-GigabitEthernet1/0/2] shutdown
   [DeviceC-GigabitEthernet1/0/2] undo stp enable
   [DeviceC-GigabitEthernet1/0/2] port link-type trunk
   [DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/2] quit
   ```

3. Configure smart link group 1:

   # Create smart link group 1.

   ```
   [DeviceC] smart-link group 1
   ```

   # Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

   ```
   [DeviceC-smlk-group1] protected-vlan reference-instance 1
   ```

   # Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

   ```
   [DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
   [DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
   ```

   # Enable flush update for smart link group 1, and specify VLAN 10 as the control VLAN.

   ```
   [DeviceC-smlk-group1] flush enable control-vlan 10
   ```

```
[DeviceC-smlk-group1] quit
```

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Configure VLAN and MST region settings:

Create VLAN 1 through VLAN 20.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 20
 Please wait... Done.
```

Map these VLANs to MSTI 1.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 20
```

Activate MST region configuration.

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Shut down GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] shutdown
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port, and assign the port to VLAN 1 through VLAN 20.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] shutdown
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] quit
```

3. Configure smart link group 1:

Create smart link group 1.

```
[DeviceD] smart-link group 1
```

Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

```
[DeviceD-smlk-group1] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

```
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 slave
```

Enable flush update for smart link group 1, and specify VLAN 20 as the control VLAN.

```
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit
```

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

Configuring Device B

1. Create VLAN 1 through VLAN 20.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 20 as the receive control VLAN.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 20
```

```
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/3] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

Configuring Device E

1. Create VLAN 1 through VLAN 20.

```
<DeviceE> system-view
[DeviceE] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceE-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Disable the spanning tree feature.

```
[DeviceE-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceE-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Disable the spanning tree feature.

```
[DeviceE-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 20 as the receive control VLAN.

```
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
[DeviceE-GigabitEthernet1/0/3] quit
```

Configuring Device A

1. Create VLAN 1 through VLAN 20.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLANs 1 through 20.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

   # Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
```

   # Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Use the **display smart-link group** command to display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: NONE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   2           18:37:20 2013/02/21

 GigabitEthernet1/0/2      SLAVE   STANDBY  2           17:45:20 2013/02/21
```

The output shows that GigabitEthernet 1/0/1 on Device C is active to forward user traffic after multiple uplink switchovers.

Use the **display smart-link flush** command to display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                          : 2
 Receiving interface of the last flush packet    : GigabitEthernet1/0/3
 Receiving time of the last flush packet         : 18:37:21 2013/02/21
 Device ID of the last flush packet              : 000f-e23d-5af0
```

```
Control VLAN of the last flush packet              : 10
```

Configuration files

- Device A:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
```

- Device B:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 20
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10
#
```

- Device C:

```
#
vlan 1
#
vlan 2 to 20
```

```
#
stp region-configuration
 instance 1 vlan 1 to 20
 active region-configuration
#
smart-link group 1
 protected-vlan reference-instance 1
 flush enable control-vlan 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 master
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
#
```

- Device D:

```
#
vlan 1
#
vlan 2 to 20
#
stp region-configuration
 instance 1 vlan 1 to 20
 active region-configuration
#
smart-link group 1
 protected-vlan reference-instance 1
 flush enable control-vlan 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 master
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
#
```

- Device E:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 20
#
```

Example: Configuring multi-smart link group load sharing

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

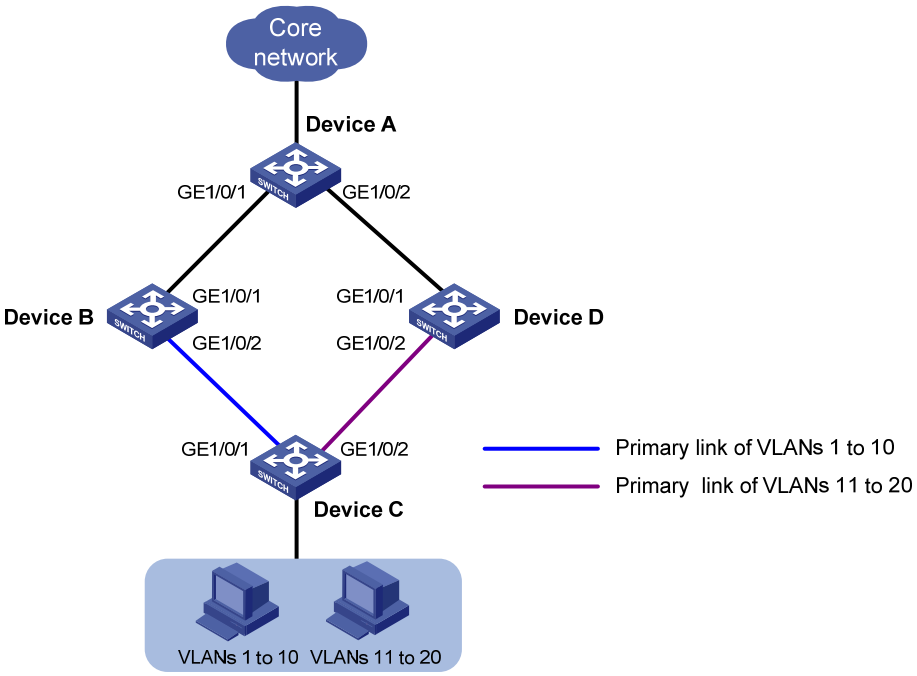
As shown in Figure 203, traffic of VLANs 1 through 20 on Device C is dually uplinked to Device A by Device B and Device D.

Configure multiple smart link groups on Device C to meet the following requirements:

- Traffic of VLANs 1 through 10 is uplinked to Device A by Device B. Traffic of VLANs 11 through 20 is uplinked to Device A by Device D.
- When the primary link of a smart link group fails, the secondary link immediately takes over to forward user traffic to implement dual uplink backup.

- When the primary link recovers, user traffic is immediately switched back to the primary link of the smart link group. Both links forward user traffic to implement load sharing.

Figure 203 Network diagram



Requirements analysis

In this example, to enable Device C to forward traffic of VLANs 1 through 10 through Device B and traffic of VLANs 11 through 20 through Device D, do the following:

- Configure GigabitEthernet 1/0/1 as the primary port for smart link group 1.
- Configure GigabitEthernet 1/0/2 as the primary port for smart link group 2 on Device C.

To make sure user traffic can be switched back to the primary link of a smart link group when the link recovers from a failure, enable role preemption for both smart link groups.

Configuration restrictions and guidelines

When you configure multi-smart link group load sharing, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in the forwarding state when a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- Make sure the receive control VLAN configured on the associated device is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.

Configuration procedures

Configuring Device C

1. Configure VLAN and MST region settings:

   # Create VLAN 1 through VLAN 20.

   ```
   <DeviceC> system-view
   [DeviceC] vlan 1 to 20
    Please wait... Done.
   ```

   # Map VLANs 1 through 10 to MSTI 1, and VLANs 11 through 20 to MSTI 2.

   ```
   [DeviceC] stp region-configuration
   [DeviceC-mst-region] instance 1 vlan 1 to 10
   [DeviceC-mst-region] instance 2 vlan 11 to 20
   ```

   # Activate MST region configuration.

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

   # Shut down GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/1
   [DeviceC-GigabitEthernet1/0/1] shutdown
   ```

   # Disable the spanning tree feature on the port.

   ```
   [DeviceC-GigabitEthernet1/0/1] undo stp enable
   ```

   # Configure the port as a trunk port, and assign the port to VLAN 1 through VLAN 20.

   ```
   [DeviceC-GigabitEthernet1/0/1] port link-type trunk
   [DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

   ```
   [DeviceC] interface gigabitethernet 1/0/2
   [DeviceC-GigabitEthernet1/0/2] shutdown
   [DeviceC-GigabitEthernet1/0/2] undo stp enable
   [DeviceC-GigabitEthernet1/0/2] port link-type trunk
   [DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
    Please wait... Done.
   [DeviceC-GigabitEthernet1/0/2] quit
   ```

3. Configure smart link group 1:

   # Create smart link group 1.

   ```
   [DeviceC] smart-link group 1
   ```

   # Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

   ```
   [DeviceC-smlk-group1] protected-vlan reference-instance 1
   ```

   # Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

   ```
   [DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
   [DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
   ```

   # Enable role preemption in smart link group 1.

```
[DeviceC-smlk-group1] preemption mode role
```

Enable flush update for smart link group 1, and specify VLAN 10 as the control VLAN.

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

4. Configure smart link group 2:

Create smart link group 2.

```
[DeviceC] smart-link group 2
```

Configure all VLANs mapped to MSTI 2 as the protected VLANs for smart link group 2.

```
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

Configure GigabitEthernet 1/0/1 as the secondary port and GigabitEthernet 1/0/2 as the primary port for smart link group 2.

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
```

Enable role preemption in smart link group 2.

```
[DeviceC-smlk-group2] preemption mode role
```

Enable flush update for smart link group 2, and specify VLAN 20 as the control VLAN.

```
[DeviceC-smlk-group2] flush enable control-vlan 20
[DeviceC-smlk-group2] quit
```

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device B

1. Create VLAN 1 through VLAN 20.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
```

```
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Create VLAN 1 through VLAN 20.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 20.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/2] quit
```

Configuring Device A

1. Create VLAN 1 through VLAN 20.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 20
 Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLAN 1 through VLAN 20.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
```

```
 Please wait... Done.
```

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs on the ports.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way you configure GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Shut down GigabitEthernet 1/0/1 on Device C, and display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  DOWN     0           NA

 GigabitEthernet1/0/2      SLAVE   ACTVIE   1           17:45:20 2013/02/21


 Smart link group 2 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 20
 Protected VLAN: Reference Instance 2
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/2      MASTER  ACTVIE   0           NA

 GigabitEthernet1/0/1      SLAVE   DOWN     0           NA
```

The output shows the following:

- A link switchover occurred in smart link group 1.
- No link switchover has occurred in smart link group 2.

Bring up GigabitEthernet 1/0/1 on Device C, and display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   1           17:50:20 2013/02/21

 GigabitEthernet1/0/2      SLAVE   STANDBY  1           17:45:20 2013/02/21


 Smart link group 2 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 20
 Protected VLAN: Reference Instance 2
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/2      MASTER  ACTVIE   0           NA

 GigabitEthernet1/0/1      SLAVE   STANDBY  0           NA
```

The output shows the following:

- The primary link of smart link group 1 is active to forward user traffic.
- No link switchover has occurred in smart link group 2.

Display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                          : 1
 Receiving interface of the last flush packet    : GigabitEthernet1/0/2
 Receiving time of the last flush packet         : 16:25:21 2013/02/21
 Device ID of the last flush packet              : 000f-e23d-5af0
 Control VLAN of the last flush packet           : 10
```

Configuration files

- Device A:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
```

```
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
```

- Device B:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10 20
#
```

- Device C:

```
#
vlan 1
#
vlan 2 to 20
#
stp region-configuration
 instance 1 vlan 1 to 10
 instance 2 vlan 11 to 20
 active region-configuration
#
smart-link group 1
 preemption mode role
 protected-vlan reference-instance 1
 flush enable control-vlan 10
smart-link group 2
 preemption mode role
 protected-vlan reference-instance 2
 flush enable control-vlan 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
```

```
 port smart-link group 1 master
 port smart-link group 2 slave
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
 port smart-link group 2 master
#
```

- Device D:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10 20
#
```

Monitor Link configuration examples

This chapter provides Monitor Link configuration examples.

Monitor Link works together with Layer 2 topology protocols to adapt the up/down state of a downlink port to the state of an uplink port. This feature enables fast link switchover on a downstream device in response to the uplink state change on its upstream device.

General configuration restrictions and guidelines

Make sure the port you want to configure as a monitor link group member port is not a member of any aggregation group or service loopback group.

Example: Configuring Monitor Link

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

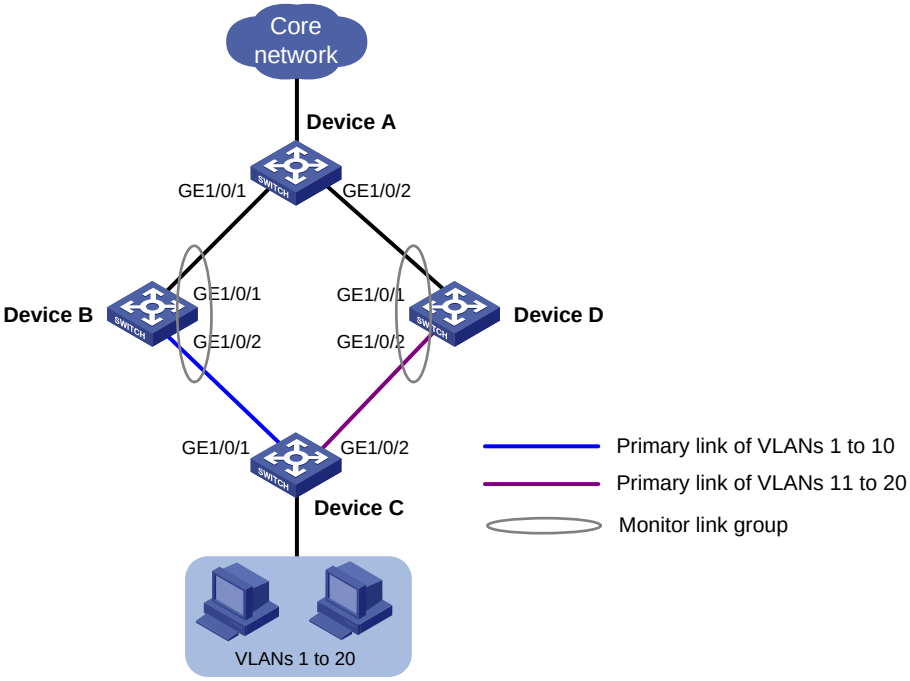
Network requirements

As shown in Figure 204, traffic of VLANs 1 through 10 and VLANs 11 through 20 on Device C is dually uplinked to Device A through Device B and Device D.

Configure multiple smart link groups on Device C and configure Monitor Link on Device B and Device D to meet the following requirements:

- Traffic of VLANs 1 through 10 is uplinked to Device A by Device B. Traffic of VLANs 11 through 20 is uplinked to Device A by Device D.
- When one forwarding link fails, user traffic is immediately switched to another link to implement dual uplink backup.
- When the link between Device A and Device B (or Device D) fails, Device C can detect the link fault and perform uplink switchover in the smart link group.

Figure 204 Network diagram



Requirements analysis

For more information about requirements analysis for configuring multiple smart link groups, see "Smart Link configuration examples."

Configuration restrictions and guidelines

When you configure Monitor Link, follow these restrictions and guidelines:

- To avoid undesired down/up state changes on the downlink ports, configure uplink ports prior to configuring downlink ports.
- For more information about configuration restrictions and guidelines for configuring multiple smart link groups, see "Smart Link configuration examples."

Configuration procedures

Configuring Smart Link

For information about smart link group configurations on Device A through Device D, see "Smart Link configuration examples."

Configuring Monitor Link

1. Configure Device B:

   # Create monitor link group 1.

   ```
   <DeviceB> system-view
   [DeviceB] monitor-link group 1
   ```

Configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceB-mtlk-group-1] quit
```

2. Configure Device D:

Create monitor link group 1.

```
<DeviceD> system-view
[DeviceD] monitor-link group 1
```

Configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit
```

Verifying the configuration

When GigabitEthernet 1/0/2 on Device A goes down due to a link fault, display information about monitor link group 1 on Device B.

```
[DeviceB] display monitor-link group 1
 Monitor link group 1 information:
 Group status: UP
 Last-up-time: 16:37:20 2013/02/21
 Last-down-time: -
 Member                    Role     Status
 ----------------------------------------
 GigabitEthernet1/0/1      UPLINK   UP
 GigabitEthernet1/0/2      DOWNLINK UP
```

The output shows that both ports in monitor link group 1 are up.

Display information about monitor link group 1 on Device D.

```
[DeviceD] display monitor-link group 1
 Monitor link group 1 information:
 Group status: DOWN
 Last-up-time: 16:37:27 2013/02/21
 Last-down-time: 16:47:19 2013/02/21
 Member                    Role     Status
 ----------------------------------------
 GigabitEthernet1/0/1      UPLINK   DOWN
 GigabitEthernet1/0/2      DOWNLINK DOWN
```

The output shows that both ports in monitor link group 1 go down because Device D detects that GigabitEthernet 1/0/2 on Device A is down.

Display smart link group information on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
```

```
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 1
Member                    Role    State    Flush-count Last-flush-time
--------------------------------------------------------------------------------
GigabitEthernet1/0/1      MASTER  ACTVIE   0           NA

GigabitEthernet1/0/2      SLAVE   DOWN     0           NA


Smart link group 2 information:
Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 20
Protected VLAN: Reference Instance 2
Member                    Role    State    Flush-count Last-flush-time
--------------------------------------------------------------------------------
GigabitEthernet1/0/2      MASTER  DOWN     0           NA

GigabitEthernet1/0/1      SLAVE   ACTVIE   1           16:47:20 2013/02/21
```

The output shows the following:

- In smart link group 2, GigabitEthernet 1/0/1 has taken over the master role because Device C detects the link failure between Device A and Device D.
- No link switchover has occurred in smart link group 1.

Configuration files

For information about the smart link group configuration files on Device A through Device D, see "Smart Link configuration examples."

- Device B:

```
#
monitor-link group 1
#
interface GigabitEthernet1/0/1
 port monitor-link group 1 uplink
#
interface GigabitEthernet1/0/2
 port monitor-link group 1 downlink
#
```

- Device D:

```
#
monitor-link group 1
#
interface GigabitEthernet1/0/1
 port monitor-link group 1 uplink
#
```

```
interface GigabitEthernet1/0/2
 port monitor-link group 1 downlink
#
```

Spanning tree configuration examples

This chapter provides spanning tree configuration examples.

General configuration restrictions and guidelines

STP is mutually exclusive with any of the following functions on a port:

- Service loopback
- Rapid Ring Protection Protocol (RRPP)
- Smart Link
- BPDU tunneling for STP

Example: Configuring MSTP

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 205:

- Device A and Device B are at the distribution layer.
- Device C, Device D, and Device E are at the access layer.

To eliminate Layer 2 loops and implement load sharing for redundant links, configure MSTP so that:

- No Layer 2 loops exist in the network.
- Packets from different VLANs are forwarded along different MSTIs:
  - Packets from VLAN 10 are forwarded along MSTI 1.
  - Packets from VLAN 20 are forwarded along MSTI 0.
  - Packets from VLAN 30 are forwarded along MSTI 2.
- The MSTI to which each VLAN is mapped is as shown in Figure 206.

Figure 205 Network diagram

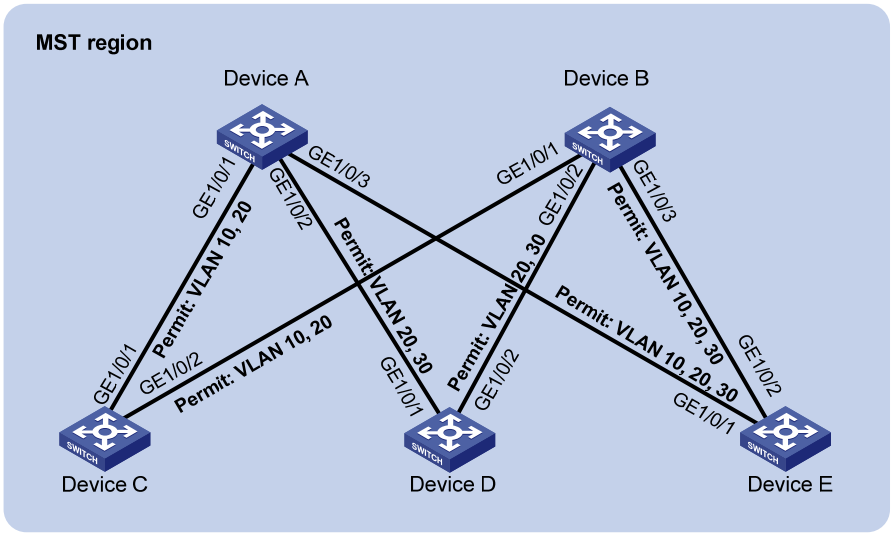
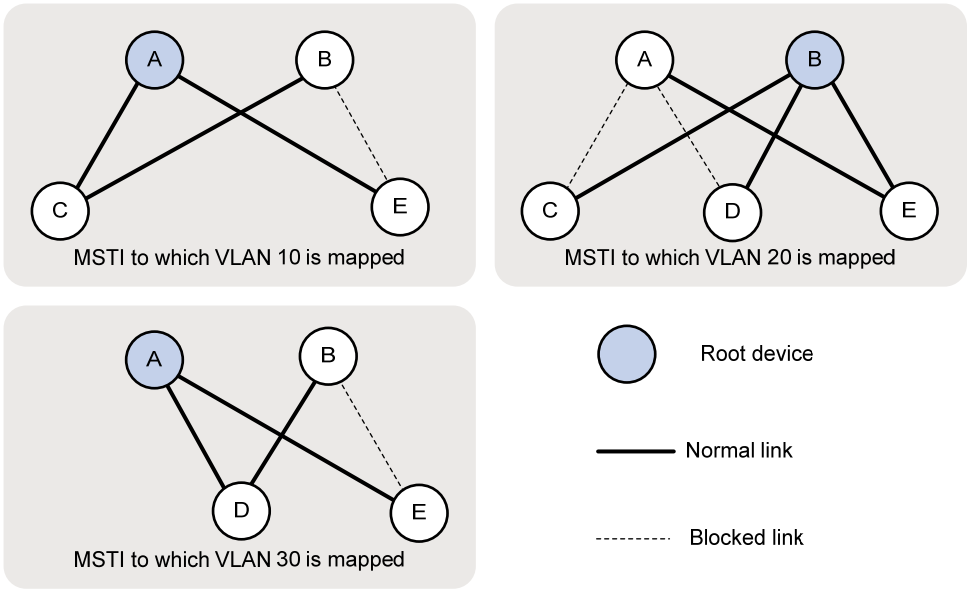


Figure 206 MSTI to which each VLAN is mapped



Requirements analysis

To forward packets from different VLANs along different physical links, you can configure different path costs for a port in different MSTIs. In this example, the path cost calculation standard is **legacy** for all devices, and the default path cost of each port is 20.

Configuration restrictions and guidelines

When you configure MSTP, follow these restrictions and guidelines:

- Two or more spanning tree devices belong to the same MST region only if both of the following are true:

    - The devices are configured to have the same format selector (0 by default, not configurable), MST region name, MST region revision level, and VLAN-to-instance mappings in the MST region.
    - The devices are connected through physical links.
- You can use the **stp mcheck** command in system view or port view. Using the **stp mcheck** command in system view takes effect on all ports. Using the **stp mcheck** command in port view takes effect on only the port.

Configuration procedures

Configuring VLANs and ports

As shown in Figure 205:

- Create VLANs 10, 20, and 30 on Device A, Device B, and Device E.
- Create VLANs 10 and 20 on Device C.
- Create VLANs 20 and 30 on Device D.

Configure the ports as follows:

- Configure each port as a trunk port.
- Assign the port to the corresponding VLANs.
- Enable the spanning tree protocol on the port.

By default, the spanning tree protocol is enabled on a port. The VLAN and port configuration procedures on each device are similar.

The VLAN and port configurations on Device A are as follows:

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] quit
[DeviceA] vlan 30
[DeviceA-vlan30] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceA-GigabitEthernet1/0/1] stp enable
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 20 30
[DeviceA-GigabitEthernet1/0/2] stp enable
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10 20 30
```

```
[DeviceA-GigabitEthernet1/0/3] stp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring Device A

Configure the MST region as follows:

- Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.
- Map VLAN 10, VLAN 20, and VLAN 30 to MSTI 1, MSTI 0, and MSTI 2, respectively. By default, all VLANs are mapped to MSTI 0.
- Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
<DeviceA> system-view
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 0 vlan 20
[DeviceA-mst-region] instance 2 vlan 30
[DeviceA-mst-region] revision-level 0
```

Display the MST region configurations that are to be activated. HP recommends that you use the **check region-configuration** command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

```
[DeviceA-mst-region] check region-configuration
```

Activate the MST region configuration.

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

Configure Device A as the primary root bridge of MSTI 1 and MSTI 2.

```
[DeviceA] stp instance 1 root primary
[DeviceA] stp instance 2 root primary
```

Configure Device A as a secondary root bridge of MSTI 0.

```
[DeviceA] stp instance 0 root secondary
```

Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceA] stp mode mstp
```

Enable the spanning tree protocol globally.

```
[DeviceA] stp enable
```

Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.

```
[DeviceA] stp mcheck
```

Configuring Device B

Configure the MST region as follows:

- Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.
- Map VLAN 10, VLAN 20, and VLAN 30 to MSTI 1, MSTI 0, and MSTI 2, respectively. By default, all VLANs are mapped to MSTI 0.
- Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
<DeviceB> system-view
[DeviceB] stp region-configuration
```

```
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 0 vlan 20
[DeviceB-mst-region] instance 2 vlan 30
[DeviceB-mst-region] revision-level 0
```

Display the MST region configurations that are to be activated. HP recommends that you use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

```
[DeviceB-mst-region] check region-configuration
```

Activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
# Configure Device B as the primary root bridge of MSTI 0.
[DeviceB] stp instance 0 root primary
```

Configure Device B as a secondary root bridge of MSTI 1 and MSTI 2.

```
[DeviceB] stp instance 1 root secondary
[DeviceB] stp instance 2 root secondary
```

Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceB] stp mode mstp
```

Enable the spanning tree protocol globally.

```
[DeviceB] stp enable
```

Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceB] stp mcheck
```

Configuring Device C

Configure the MST region as follows:

- Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.
- Map VLAN 10, VLAN 20, and VLAN 30 to MSTI 1, MSTI 0, and MSTI 2, respectively. By default, all VLANs are mapped to MSTI 0.
- Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 0 vlan 20
[DeviceC-mst-region] instance 2 vlan 30
[DeviceC-mst-region] revision-level 0
```

Display the MST region configurations that are to be activated. HP recommends that you use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

```
[DeviceC-mst-region] check region-configuration
```

Activate the MST region configuration.

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

Set the path cost of port GigabitEthernet 1/0/1 in MSTI 1 to 15.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] stp instance 1 cost 15
[DeviceC-GigabitEthernet1/0/1] quit
```

Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceC] stp mode mstp
```

Enable the spanning tree protocol globally.

```
[DeviceC] stp enable
```

Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceC] stp mcheck
```

Configuring Device D

Configure the MST region as follows:

- Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.
- Map VLAN 10, VLAN 20, and VLAN 30 to MSTI 1, MSTI 0, and MSTI 2, respectively. By default, all VLANs are mapped to MSTI 0.
- Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 0 vlan 20
[DeviceD-mst-region] instance 2 vlan 30
[DeviceD-mst-region] revision-level 0
```

Display the MST region configurations that are to be activated. HP recommends that you use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

```
[DeviceD-mst-region] check region-configuration
```

Activate the MST region configuration.

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

Set the path cost of port GigabitEthernet 1/0/1 in MSTI 2 to 15. The path cost is an important factor in spanning tree calculation.

Setting different path costs for a port in different MSTIs does the following:

- Allows traffic flows from different VLANs to be forwarded along different physical links.
- Enables VLAN-based load balancing.

In this example:

- The path cost calculation standard is **legacy** for all ports.
- Each port is a single port without the link aggregation configuration.
- Each port has a link speed of 1000 Mbps.

As a result, the default path cost of each port is 20.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] stp instance 2 cost 15
```

```
[DeviceD-GigabitEthernet1/0/1] quit
```

Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceD] stp mode mstp
```

Enable the spanning tree protocol globally.

```
[DeviceD] stp enable
```

Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceD] stp mcheck
```

Configuring Device E

Configure the MST region as follows:

- Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.
- Map VLAN 10, VLAN 20, and VLAN 30 to MSTI 1, MSTI 0, and MSTI 2, respectively. By default, all VLANs are mapped to MSTI 0.
- Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
<DeviceE> system-view
[DeviceE] stp region-configuration
[DeviceE-mst-region] region-name example
[DeviceE-mst-region] instance 1 vlan 10
[DeviceE-mst-region] instance 0 vlan 20
[DeviceE-mst-region] instance 2 vlan 30
[DeviceE-mst-region] revision-level 0
```

Display the MST region configurations that are to be activated. HP recommends that you use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

```
[DeviceE-mst-region] check region-configuration
```

Activate the MST region configuration.

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

Set the path cost of port GigabitEthernet 1/0/2 of Device E in MSTI 0 to 15. The path cost is an important factor in spanning tree calculation.

Setting different path costs for a port in different MSTIs does the following:

- Allows traffic flows from different VLANs to be forwarded along different physical links.
- Enables VLAN-based load balancing.

In this example:

- The path cost calculation standard is **legacy** for all ports.
- Each port is a single port without the link aggregation configuration.
- Each port has a link speed of 1000 Mbps.

As a result, the default path cost of each port is 20.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] stp instance 0 cost 15
[DeviceE-GigabitEthernet1/0/2] quit
```

Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceE] stp mode mstp
```

Enable the spanning tree protocol globally.

```
[DeviceE] stp enable
```

Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceE] stp mcheck
```

Verifying the configuration

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        ALTE  DISCARDING    NONE
   0        GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
   0        GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   2        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   2        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   1        GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/3        ALTE  DISCARDING    NONE
   2        GigabitEthernet1/0/2        ROOT  FORWARDING    NONE
   2        GigabitEthernet1/0/3        ALTE  DISCARDING    NONE
```

Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/2        ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        GigabitEthernet1/0/1        DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/2        ROOT  FORWARDING    NONE
   2        GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   2        GigabitEthernet1/0/2        DESI  FORWARDING    NONE
```

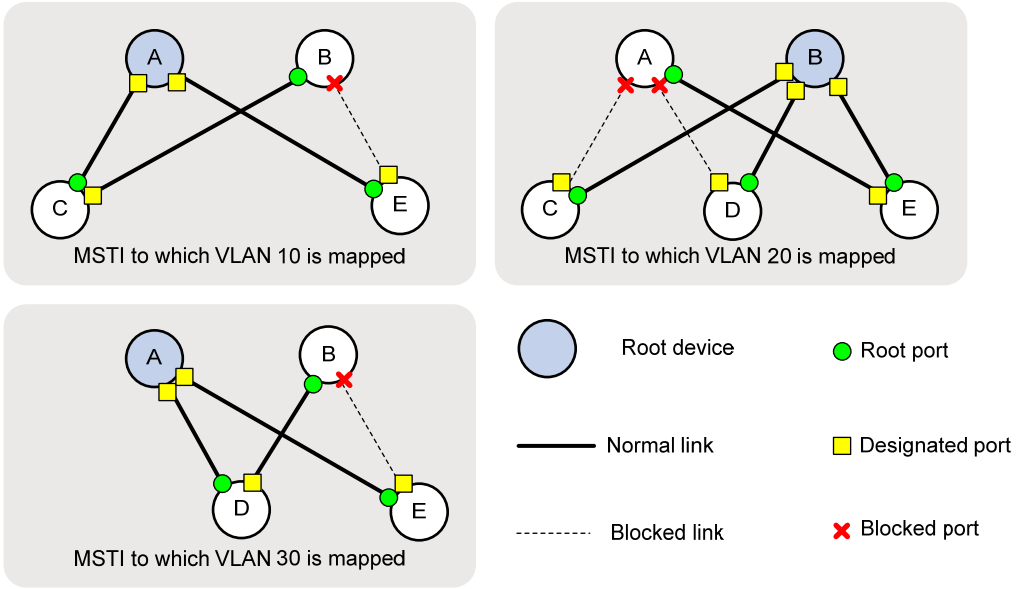
Display brief spanning tree information on Device E.

```
[DeviceE] display stp brief
```

```
MSTID      Port                      Role  STP State     Protection
  0        GigabitEthernet1/0/1      DESI  FORWARDING    NONE
  0        GigabitEthernet1/0/2      ROOT  FORWARDING    NONE
  1        GigabitEthernet1/0/1      ROOT  FORWARDING    NONE
  1        GigabitEthernet1/0/2      DESI  FORWARDING    NONE
  2        GigabitEthernet1/0/1      ROOT  FORWARDING    NONE
  2        GigabitEthernet1/0/2      DESI  FORWARDING    NONE
```

Based on the output, you can draw the MSTI to which each VLAN is mapped, as shown in Figure 207. The figure shows that the network requirements are satisfied.

Figure 207 MSTI to which each VLAN is mapped



Configuration files

- Device A:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
 stp instance 0 root secondary
 stp instance 1 root primary
 stp instance 2 root primary
```

```
 stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
#
```

- Device B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
 stp instance 0 root primary
 stp instance 1 root secondary
 stp instance 2 root secondary
 stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
#
```

- Device C:

```
#
vlan 10
#
vlan 20
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 stp instance 1 cost 15
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
```

- Device D:

```
#
vlan 20
#
vlan 30
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
```

```
 stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 stp instance 2 cost 15
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
```

- Device E:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
 stp instance 0 cost 15
#
```

Example: Configuring RSTP

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

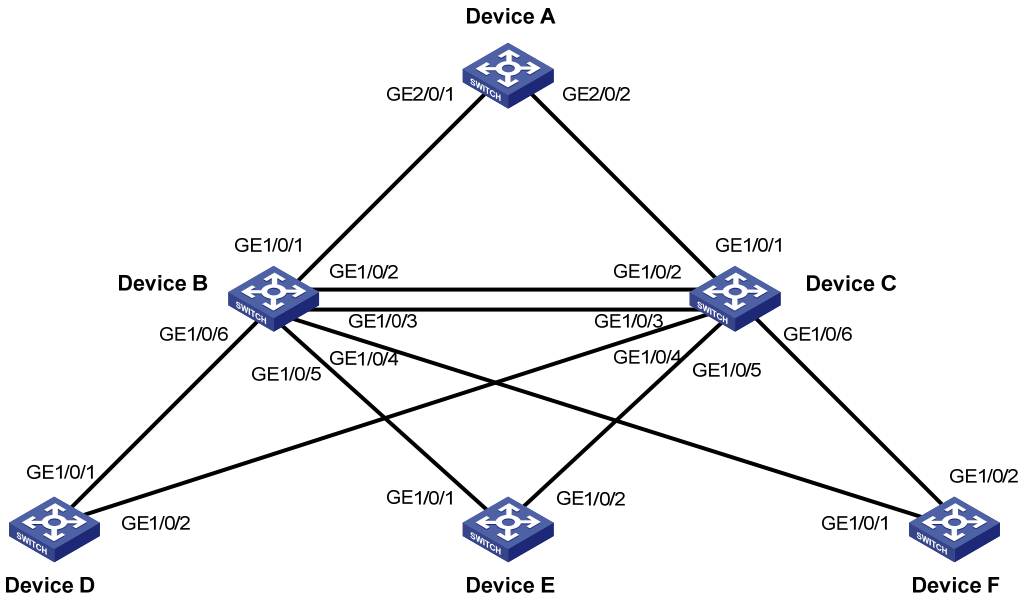
As shown in Figure 208, the LAN has multiple layers:

- Device A operates at the core layer.
- Device B and Device C operate at the distribution layer. Device C and Device B are connected through two links.
- Device D, Device E, and Device F operate at the access layer. PCs are directly connected to Device D, Device E, and Device F.
- Suppose all ports of these devices have the same path cost.

Configure RSTP to eliminate loops and implement link backup, so that:

- Device A is the root bridge. Enable root guard on the device to protect the device against configuration errors and malicious attacks.
- Device C backs up Device B. When Device B fails, Device C takes over to forward data traffic.
- Configure the ports of Device D, Device E, and Device F that directly connect to users as edge ports, and enable BPDU guard on these ports.
- Ensure network stability and protect the network against forged TC-BPDUs.

Figure 208 Network diagram



NOTE:

- Typically, Device A is a high-end or mid-range switch, for example, an HP 7500 switch.
- Typically, Device B and Device C are the HP 5800 or 5500 switches of the low-end switches.
- Typically, Device D, Device E, and Device F are the HP 3600 v2 switches of the low-end switches.
- The following section describes only the RSTP configurations.

Requirements analysis

To protect the root bridge against configuration errors and malicious attacks, enable root guard on the designated ports of Device A, Device B, and Device C.

To make Device C serve as the backup of Device B, assign Device B a higher priority than that of Device C.

To protect the network against forged TC-BPDUs, enable TC-BPDU guard on the root bridge Device A.

Configuration procedures

Configuring Device A

Set the spanning tree mode to RSTP.

```
<DeviceA> system-view
[DeviceA] stp mode rstp
```

Configure Device A as the primary root bridge.

```
[DeviceA] stp root primary
```

NOTE:

You can also configure Device A as the primary root bridge by setting the device priority to 0 by using the **stp priority 0** command.

Enable root guard on the ports connecting Device A to Device B and Device C.

```
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] stp root-protection
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] stp root-protection
[DeviceA-GigabitEthernet2/0/2] quit
```

Enable TC-BPDU guard on Device A. TC-BPDU guard is enabled by default.

```
[DeviceA] stp tc-protection enable
```

Enable RSTP globally.

```
[DeviceA] stp enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceA] stp mcheck
```

When RSTP is globally enabled, RSTP is automatically enabled on each port by default. Disable STP on the ports that do not participate in the RSTP calculation. Do not disable STP on the ports that participate in the RSTP calculation. (This examples uses GigabitEthernet 2/0/4.)

```
[DeviceA] interface GigabitEthernet 2/0/4
[DeviceA-GigabitEthernet2/0/4] undo stp enable
[DeviceA-GigabitEthernet2/0/4] quit
```

Configuring Device B

Set the spanning tree mode to RSTP.

```
<DeviceB> system-view
[DeviceB] stp mode rstp
```

Set the device priority to 4096 for Device B.

```
[DeviceB] stp priority 4096
```

Enable root guard on each designated port.

```
[DeviceB] interface GigabitEthernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] stp root-protection
[DeviceB-GigabitEthernet1/0/4] quit
[DeviceB] interface GigabitEthernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] stp root-protection
[DeviceB-GigabitEthernet1/0/5] quit
[DeviceB] interface GigabitEthernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] stp root-protection
[DeviceB-GigabitEthernet1/0/6] quit
```

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.

```
[DeviceB] stp enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceB] stp mcheck
```

When RSTP is globally enabled, RSTP is automatically enabled on each port by default. Disable STP on the ports that do not participate in the RSTP calculation. Do not disable STP on the ports that participate in the RSTP calculation. (This example uses GigabitEthernet 1/0/8.)

```
[DeviceB] interface GigabitEthernet 1/0/8
[DeviceB-GigabitEthernet1/0/8] undo stp enable
[DeviceB-GigabitEthernet1/0/8] quit
```

Configuring Device C

Set the spanning tree mode to RSTP.

```
<DeviceC> system-view
[DeviceC] stp mode rstp
```

Set the device priority to 8192 for Device C, so that Device C serves as the backup of Device B.

```
[DeviceC] stp priority 8192
```

Enable root guard on each designated port.

```
[DeviceC] interface GigabitEthernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] stp root-protection
[DeviceC-GigabitEthernet1/0/4] quit
[DeviceC] interface GigabitEthernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] stp root-protection
[DeviceC-GigabitEthernet1/0/5] quit
[DeviceC] interface GigabitEthernet 1/0/6
[DeviceC-GigabitEthernet1/0/6] stp root-protection
[DeviceC-GigabitEthernet1/0/6] quit
```

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.

```
[DeviceC] stp enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceC] stp mcheck
```

When RSTP is globally enabled, RSTP is automatically enabled on each port by default. Disable STP on the ports that do not participate in the RSTP calculation. Do not disable STP on the ports that participate in the RSTP calculation. (This example uses GigabitEthernet 1/0/8.)

```
[DeviceC] interface GigabitEthernet 1/0/8
[DeviceC-GigabitEthernet1/0/8] undo stp enable
[DeviceC-GigabitEthernet1/0/8] quit
```

Configuring Device D

Set the spanning tree mode to RSTP.

```
<DeviceD> system-view
[DeviceD] stp mode rstp
```

Configure the ports directly connecting to users as edge ports, and enable BPDU guard on them. (This example uses GigabitEthernet 1/0/4.)

```
[DeviceD] interface GigabitEthernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] stp edged-port enable
[DeviceD-GigabitEthernet1/0/4] quit
[DeviceD] stp bpdu-protection
```

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.

```
[DeviceD] stp enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceD] stp mcheck
```

When RSTP is globally enabled, RSTP is automatically enabled on each port by default. Disable STP on the ports that do not participate in the RSTP calculation. Do not disable STP on the ports that participate in the RSTP calculation. (This examples uses GigabitEthernet 1/0/3.)

```
[DeviceD] interface GigabitEthernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] quit
```

Configuring Device E and Device F

Configure Device E and Device F in the same way Device D is configured.

Verifying the configuration

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

Configuration files

- Device A:

```
#
 stp mode rstp
 stp instance 0 root primary
 stp enable
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet2/0/4
 port link-mode bridge
 stp disable
#
```

- Device B:

```
#
 stp mode rstp
 stp instance 0 priority 4096
 stp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp root-protection
#
```

```
interface GigabitEthernet1/0/5
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 stp disable
#
```

- Device C:

```
#
 stp mode rstp
 stp instance 0 priority 8192
 stp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 stp disable
#
```

- Device D:

```
#
 stp mode rstp
 stp bpdu-protection
 stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp edged-port enable
#
```

Example: Configuring interoperability with a third-party device that uses a private key to calculate the configuration digest

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

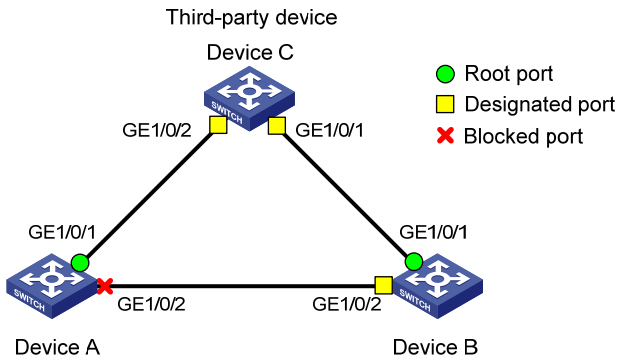
Network requirements

The configuration digest is 16 bytes and is the result calculated by using the HMAC-MD5 algorithm based on VLAN-to-instance mappings. Because spanning tree implementations vary with vendors, the configuration digests calculated through private keys are different. As a result, devices from different vendors in the same MST region cannot communicate with each other.

As shown in Figure 209, Device A, Device B, and Device C are interconnected, and they are in the same MST region. Device C is a third-party device configured as the root bridge, and it uses a private key to calculate the configuration digest.

Enable digest snooping on the ports of Device A and Device B that connect to Device C, so that the three devices can communicate with one another.

Figure 209 Network diagram



Configuration restrictions and guidelines

When you configure digest snooping, follow these restrictions and guidelines:

- HP recommends that you enable digest snooping first and then the spanning tree protocol. To avoid traffic interruption, do not configure digest snooping when the network is already working well.

- To make digest snooping take effect, you must enable the feature both globally and on the involved ports. HP recommends that you enable digest snooping on all involved ports first and then globally. Doing so makes digest snooping take effect on all configured ports at the same time and reduces impact on the network.
- To avoid loops, do not enable digest snooping on MST region boundary ports.
- When digest snooping takes effect on ports, the ports do not verify whether devices are in the same MST region by comparing configuration digests. You must make sure the connected devices have the same VLAN-to-instance mappings.

Configuration procedures

Completing basic MSTP configurations on the devices

Details are not shown.

Configuring Device A

Enable digest snooping on port GigabitEthernet 1/0/1, and enable digest snooping globally. To make digest snooping take effect on a port, you must enable this feature both globally and on the port.

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

Configuring Device B

Enable digest snooping on port GigabitEthernet 1/0/1, and enable digest snooping globally. To make digest snooping take effect on a port, you must enable this feature both globally and on the port.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] stp config-digest-snooping
```

Verifying the configuration

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

Configuration files

- Device A:

```
#
 stp config-digest-snooping
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp config-digest-snooping
#
```

- Device B:

```
#
 stp config-digest-snooping
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp config-digest-snooping
#
```

Example: Configuring interoperability with an upstream third-party device that uses a private MSTP implementation

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

The designated port of an RSTP, PVST, or MSTP device can implement rapid state transition through exchanging Proposal and Agreement packets with the root port of a downstream device.

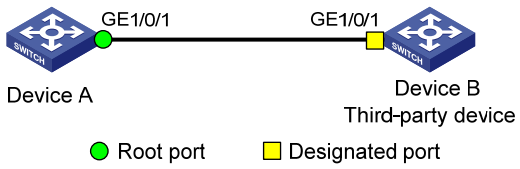
When the downstream device is an HP device and is connected to a third-party upstream device that has a private spanning tree implementation, the rapid state transition implementation might be limited.

As shown in Figure 210:

- Device A is an HP device.
- Device A connects to a third-party device (Device B) that has a private spanning tree implementation.
- Device A and Device B are in the same MST region, and Device B is the root bridge.

Enable No Agreement Check on the port connecting Device A to Device B, so that port GigabitEthernet 1/0/1 on Device B can rapidly transit its port state.

Figure 210 Network diagram



Configuration restrictions and guidelines

To make the No Agreement Check feature take effect, enable the feature on the root port.

Configuration procedures

1. Complete basic MSTP configurations on the devices. (Details not shown.)
2. Enable No Agreement Check on port GigabitEthernet 1/0/1 of Device A.

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

Verifying the configuration

When the network is stable, use the **display stp interface** *interface-list* command to display the STP calculation status on each port.

The STP calculation status includes the following:

- The port state
- Whether the port supports rapid transition

Configuration files

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp no-agreement-check
#
```

SSH configuration examples

This chapter provides examples for configuring SSH for secure remote access and file transfer.

General configuration restrictions and guidelines

When you configure SSH, follow these restrictions and guidelines:

- When acting as an SSH server, the switch supports SSH2.0 and SSH1. When acting as an SSH client, the switch supports SSH2.0 only.
- The switch that runs Release 1208 or later versions supports SCP.

Example: Configuring the switch as an Stelnet server for password authentication

Applicable product matrix

Product series	Software version
HP 7500	Release 6620 Release 6630 Release 6700

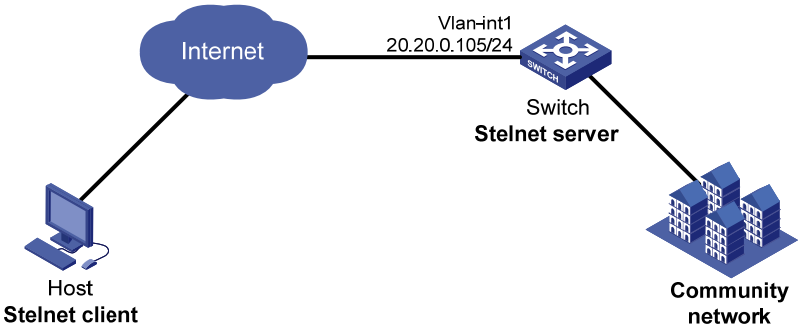
Network requirements

As shown in Figure 211, you can log in to the switch through the Stelnet client that runs on the host for configuration and management.

The switch acts as the Stelnet server to perform local password authentication.

The switch limits the number of authentication attempts to prevent malicious hacking of usernames and passwords.

Figure 211 Network diagram



Configuration restrictions and guidelines

When you configure the switch as an Stelnet server for password authentication, follow these restrictions and guidelines:

- An SSH client uses either DSA or RSA public key algorithm to authenticate the SSH server. To support SSH clients that use different types of key pairs and make sure the client can successfully log in to the server, generate both DSA and RSA key pairs on the SSH server.
- When password authentication is used, the command level accessible to the user is authorized by AAA.
- Authentication fails if the total number of authentication attempts (including both publickey and password authentication) exceeds the upper limit configured by the **ssh server authentication-retries** command. This configured upper limit takes effect only on the users at next login.

Configuration procedures

Configuring the switch

Assign an IP address to VLAN interface 1. The Stelnet client uses the IP address as the destination address of the SSH connection.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 20.20.0.105 255.255.255.0
[Switch-Vlan-interface1] quit
```

Generate RSA and DSA key pairs.

```
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
++++++++++++++++++++++++++
++++++++++++++++++++++++
++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
*
..+.++++*
```

Enable the SSH server function.

```
[Switch] ssh server enable
```

```
Info: Enable SSH server
```

Set the maximum number of SSH authentication attempts to 5.

```
[Switch] ssh server authentication-retries 5
```

Set the authentication mode for the user interface to AAA, and enable the user interface to support SSH.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
```

Create a local user **client001** with the password **aabbcc**, service type **ssh**, and user privilege level **3**.

```
[Switch] local-user client001
New local user added.
[Switch-luser-client001] password simple aabbcc
[Switch-luser-client001] service-type ssh
[Switch-luser-client001] authorization-attribute level 3
[Switch-luser-client001] quit
```

Specify the service type for the user **client001** as **Stelnet** and the authentication method as **password**.

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

Configuring the SSH client

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY Version 0.58.

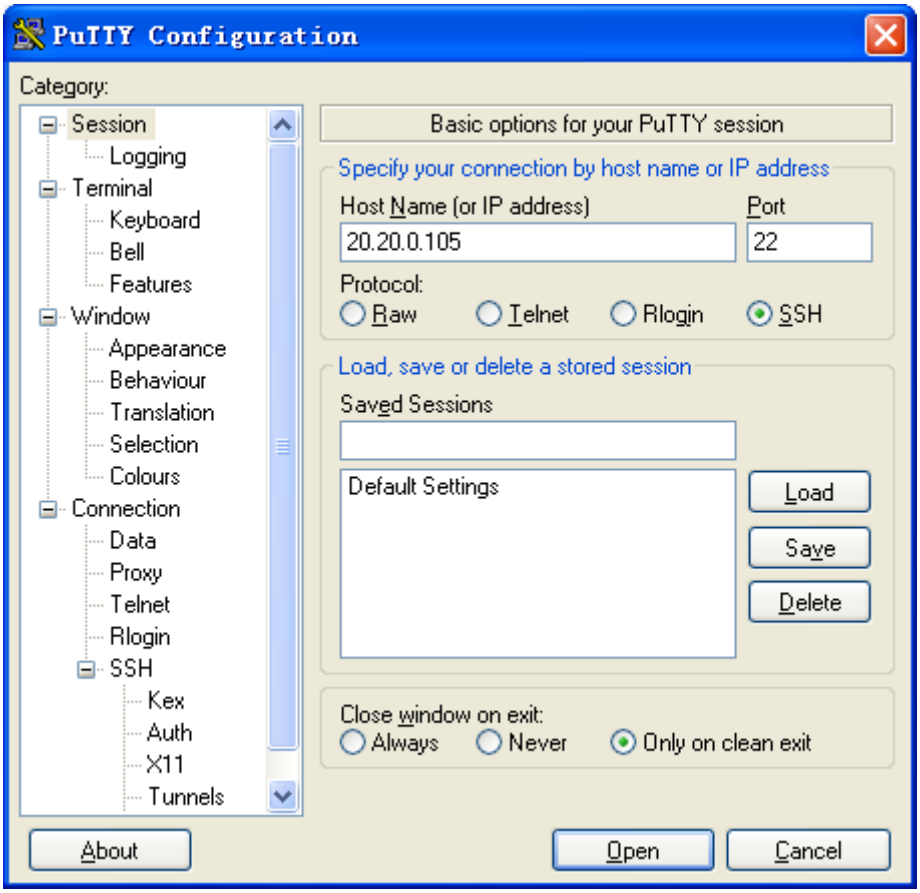
To establish a connection to the Stelnet server:

1. Launch PuTTY.exe.

   The dialog box in Figure 212 appears.

2. In the **Host Name** (or **IP address**) field, enter the IP address of the Stelnet server (20.20.0.105).

Figure 212 Specifying the Stelnet server



3. Click **Open**.

   A security alert is displayed, asking whether you trust this server and want to continue.
4. Click **Yes**.
5. Enter the username **client001** and password **aabbcc** to log in to the Stelnet server.

Verifying the configuration

Verify that you can use the username **client001** and password **aabbcc** to access the Stelnet server's CLI.

```
Login as: client001
client001@20.20.0.105's password:
******************************************************************************
* Copyright (c) 2004-2013 Hewlett-Packard Development Company,L.P.           *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

CLI configuration files

```
#
```

```
vlan 1
#
local-user client001
 password cipher $c$3$6XrvmIWDHxv6M9ykP9qJrqy9/Jlb1z8xSg==
 authorization-attribute level 3
 service-type ssh
#
interface Vlan-interface1
 ip address 20.20.0.105 255.255.255.0
#
 ssh server enable
 ssh server authentication-retries 5
 ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 15
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
#
```

Example: Configuring the switch as an Stelnet server for publickey authentication

Applicable product matrix

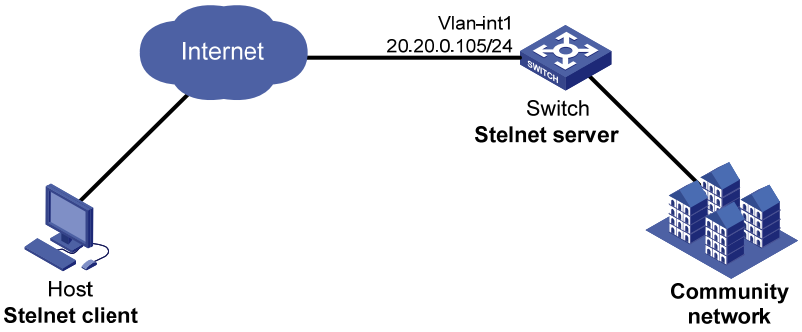
Product series	Software version
HP 7500	Release 6620 Release 6630 Release 6700

Network requirements

As shown in Figure 213, you can log in to the switch through the Stelnet client that runs on the host for configuration and management.

The switch acts as the Stelnet server and uses publickey authentication and the RSA public key algorithm.

Figure 213 Network diagram



Requirements analysis

For successful publickey authentication, do the following:

- Generate RSA key pairs on the client.
- Upload the client's host public key to the server.
- Specify the client's host public key for the SSH user on the server.

To enable the client to authenticate the server, you must also generate RSA key pairs on the server.

Configuration restrictions and guidelines

When publickey authentication is used, the command level accessible to the user is set by the **user privilege level** command on the user interface.

Configuration procedures

Configuring the Stelnet client

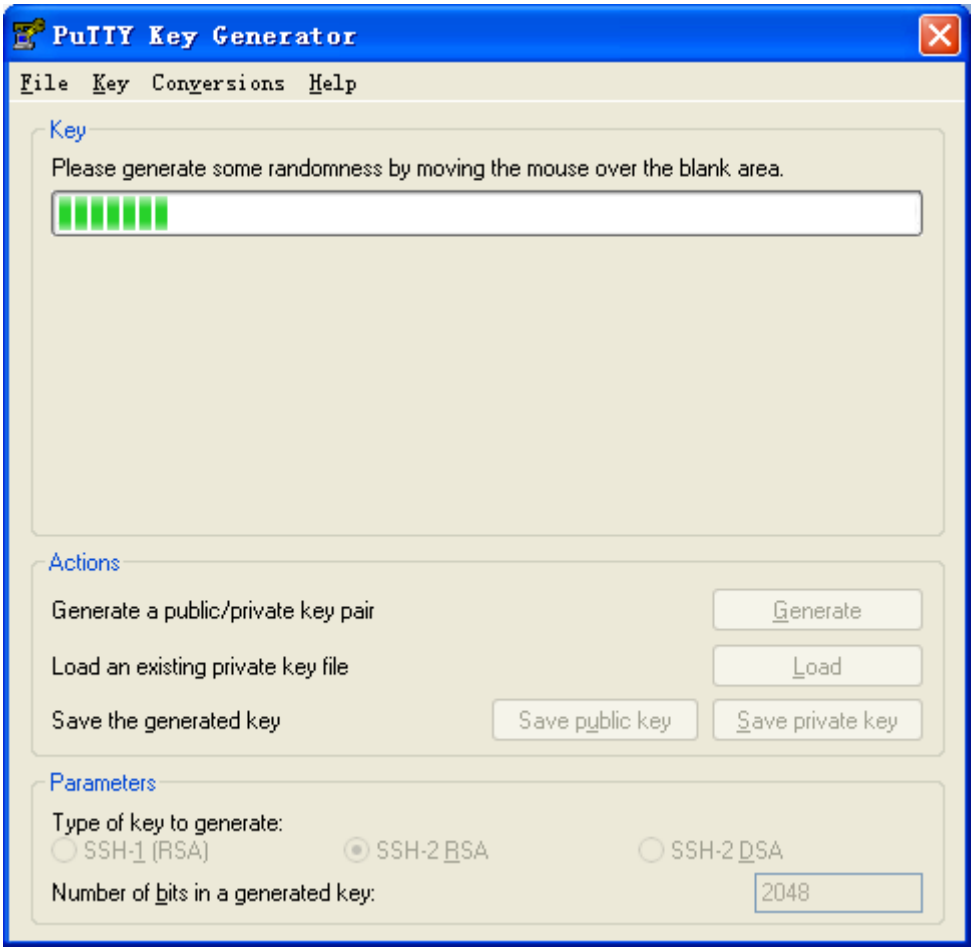
1. Run PuTTYGen.exe on the client.

   The dialog box in Figure 214 appears.
2. Select **SSH-2 RSA** and enter **2048** in the **Number of bits in a generated key** field.
3. Click **Generate**.

Figure 214 Generating the RSA key pair on the client

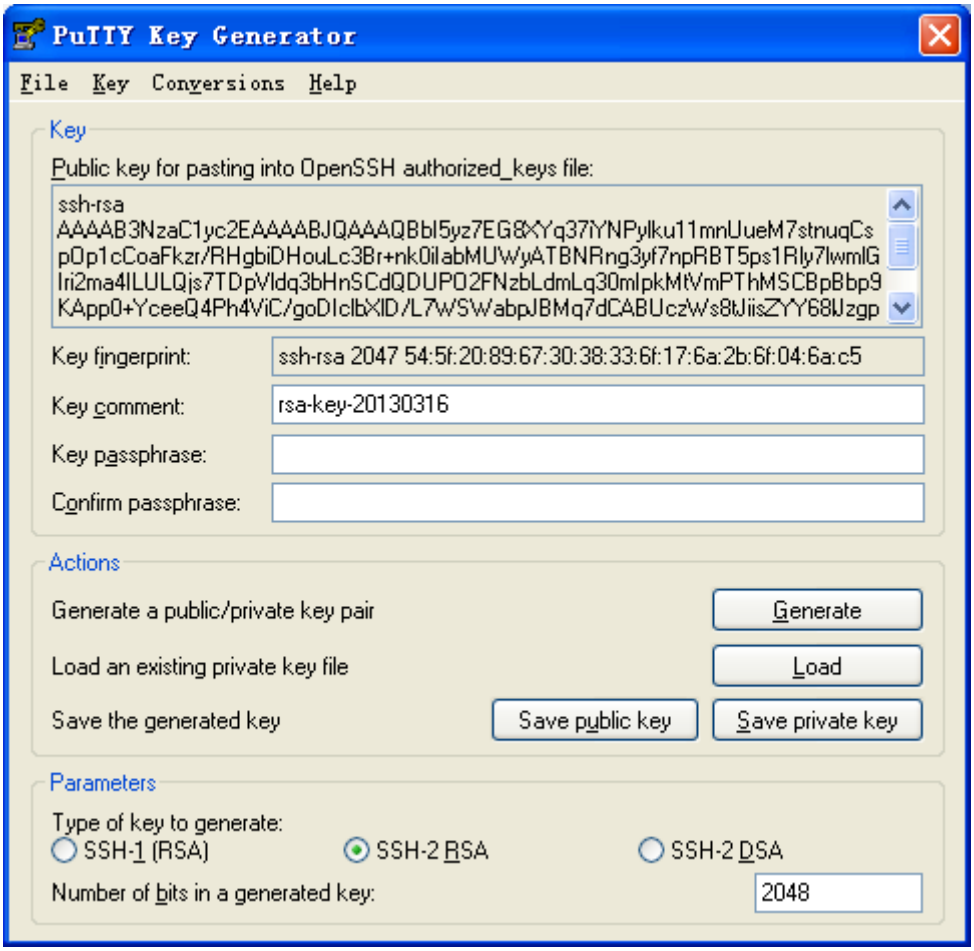
4. Continuously move the mouse, and do not place the mouse over the progress bar shown in Figure 215. Otherwise, the key pair generating progress stops.

Figure 215 Generating process



5. After the key pair is generated, save the public key:
   a. Click **Save public key**.
   b. Specify a directory (root directory of disk C in this example).
   c. Enter a file name (**key.pub** in this example).
   d. Click **Save**.

Figure 216 Saving the generated key pair



6. Click **Save private key** to save the private key.

   A confirmation dialog box appears.

7. Click **Yes**, enter a file name (**private.ppk**, in this example), and click **Save**.

Configuring the switch as an FTP server

Assign an IP address to VLAN interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 20.20.0.105 255.255.255.0
[Switch-Vlan-interface1] quit
```

Create a local user with the service type **ftp** on the switch.

```
[Switch] local-user ftp
New local user added.
[Switch-luser-ftp] password simple ftp
[Switch-luser-ftp] authorization-attribute level 3
[Switch-luser-ftp] authorization-attribute work-directory flash:/
[Switch-luser-ftp] service-type ftp
[Switch-luser-ftp] quit
```

Enable the FTP server function on the switch.

```
[Switch] ftp server enable
```

```
[Switch] quit
```

Uploading the public key file to the server

Log in to the switch from the client, and upload the public key file (**key.pub**) to the switch through FTP.

```
c:\> ftp 20.20.0.105
Connected to 20.20.0.105.
220 FTP service ready.
User(20.20.0.105:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
ftp> put key.pub
200 Port command okay.
150 Opening ASCII mode data connection for /key.pub.
226 Transfer complete.
ftp> bye
221 Server closing.
c:\
```

Configuring the switch as an Stelnet server

1. Generate the RSA key pairs.

```
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

2. Enable the SSH server function.

```
[Switch] ssh server enable
```

3. Configure the VTY user interfaces:

Enable scheme authentication.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

Enable the user interfaces to support SSH in the inbound direction.

```
[Switch-ui-vty0-15] protocol inbound ssh
```

Set the user privilege level to 3.

```
[Switch-ui-vty0-15] user privilege level 3
[Switch-ui-vty0-15] quit
```

4. Import the client's public key from the file **key.pub** and name it **Switch001**.

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

5. # Create an SSH user **client002** with the service type **ssh** and the user privilege level **3**.

```
[Switch] local-user client002
```

```
New local user added.
[Switch-luser-client002] service-type ssh
[Switch-luser-client002] authorization-attribute level 3
[Switch-luser-client002] quit
```

6. Specify the authentication method as **publickey** for the user **client002**, and assign the public key **Switch001** to the user.

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey Switch001
[Switch] quit
```

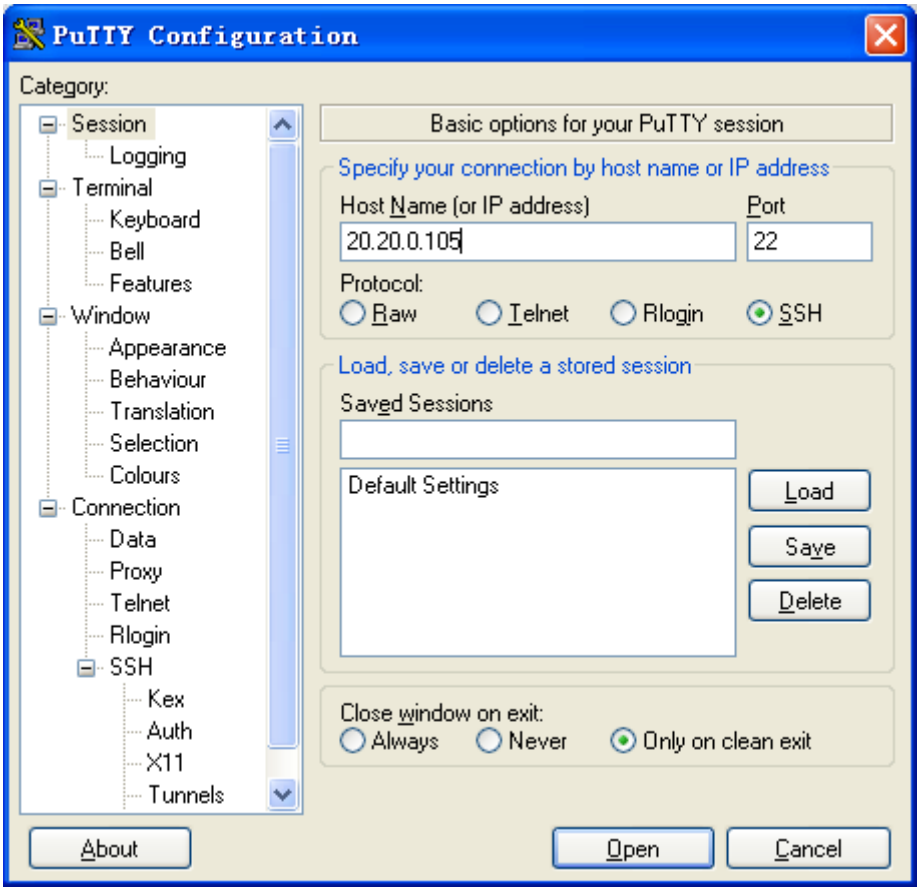
Establishing a connection to the Stelnet server

1. Launch PuTTY.exe on the Stelnet client.

   The dialog box in Figure 217 appears.

2. In the **Host Name** (or **IP address**) field, enter the IP address of the Stelnet server (22.22.0.105).

Figure 217 Specifying the Stelnet server

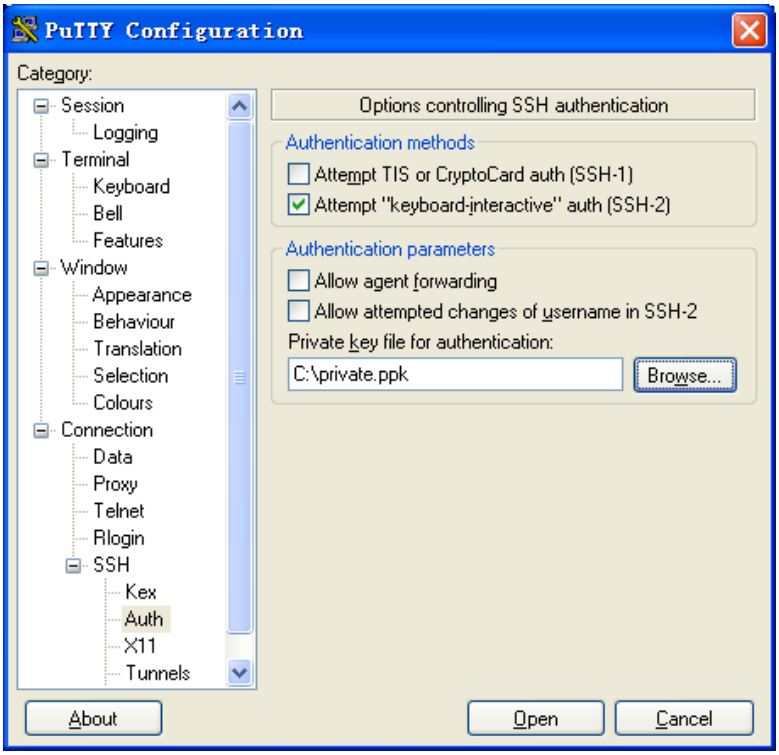


3. Select **Connection** > **SSH** > **Auth** from the navigation tree.

   The dialog box shown in Figure 218 appears.

4. Click **Browse...**.
5. Select the private key file (**private.ppk**, in this case), and click **OK**.

Figure 218 Specifying the private key file



6. Click **Open** to connect to the server.
7. Enter the username **client002** to log in to the Stelnet server.

Verifying the configuration

Verify that you can use the username **client002** to access the Stelnet server's CLI.

```
Login as: client002
Authenticating with public key “rsa-key-20130316”

******************************************************************************
* Copyright (c) 2004-2013 Hewlett-Packard Development Company,L.P..          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Switch>
```

CLI configuration files

```
#
vlan 1
#
 public-key peer Switch001
  public-key-code begin
```

```
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837BEF5D32259844
2D6753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A6627243EAD766D57AEA70B901B4B45
66D9A651B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCAF28FF21EE4EADAE6DF52001944A40414DFF2
80FF043B14838288BE7F9438DC71ABBC2C28BF78F34ADF3D1C912579A19020125
  public-key-code end
 peer-public-key end
#
local-user client002
 authorization-attribute level 3
 service-type ssh
#
local-user ftp
 password cipher $c$3$sg9WgqO1w8vnAv2FKGTOYgFJm3nn2w==
 authorization-attribute work-directory flash:/
 authorization-attribute level 3
 service-type ftp
#
interface Vlan-interface1
 ip address 20.20.0.105 255.255.255.0
#
 ssh server enable
 ssh user client002 service-type stelnet authentication-type publickey assign publickey
Switch001
#
user-interface vty 0 15
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
#
```

Example: Configuring the switch as an Stelnet client for password authentication

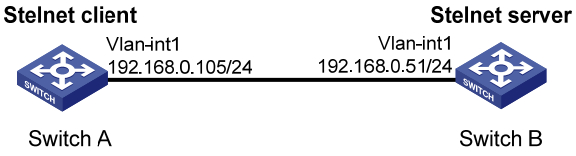
Applicable product matrix

Product series	Software version
HP 7500	Release 6620 Release 6630 Release 6700

Network requirements

As shown in Figure 219, you can log in to Switch B through the Stelnet client that runs on Switch A for configuration and management. Switch B acts as the Stelnet server and uses password authentication and DSA public key algorithm.

Figure 219 Network diagram



Requirements analysis

By default, the client supports first-time authentication. The client can access the server and save the server's host public key on the client. When accessing the server again, the client uses the saved server host public key to authenticate the server.

In a secure network, first-time authentication simplifies client configuration. However, it also brings some potential security risks.

If you disable the first-time authentication by using the **undo ssh client first-time** command, the client refuses to access the server. To enable the client to access the server, you must configure the server's host public key and specify the public key name for authentication on the client in advance.

Configuration procedures

Configuring Switch B

Assign an IP address to VLAN interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.51 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Generate a DSA key pair.

```
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
++++++++++++++++++
```

Display the DSA key pair on Switch B.

```
[SwitchB ] display public-key local dsa public

=====================================================
Time of Key pair created: 15:23:11  2012/02/26
Key name: HOST_KEY
Key type: DSA Encryption Key
=====================================================
Key code:
```

```
3082033B3082022E06072A8648CE3804013082022102820101 00F13ACC1693AFD04B9E1E8D2A9DEA
6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E6768193914B823BDF215
D0DAD7A151E434F9E128DAFB9DEFAE07874621E70D7FC4577D2851C707BC86AC0FD3829B862C5CD7
003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74DA31DA0415264F3FA3E1A6E0
F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE794C09A6C7DDE05F1E0E928E82EEA31
DB2454CD2E6866599DDF2381163734AD5C6F8A98A791BAD8942A5D12D674FCA42EA93FF7FDD23E4E
E29C35F75C8E52EF1B132073679EE2E62DF435CE35BB7F0FB756DF92A95C3652F979BD03F8D2BB62
018B021500C773218C737EC8EE993B4F2DED30F48EDACE915F0282010100D43E90A700F70A4EE08C
728A297DA04566A0A112DC49ABF51A37BBB56BFE518BBDCD71359EACE98712BEC58A261FC6D5FE78
B9A67ED494288CB5A1984CA67037A16BFC75B889829C92465BA094460D7EEF918969C0ADAE4841D1
4A880142151C394C28F2731304C456350479D62014C81F07A0BA5FD0F9301D8F9AF9F30C6D21471F
00B65714991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBCE7D283D144D4F5B5B61
B4ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA36E3DAE08B774836A3B
5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B430B003ACDEB6C9B213A
8749765992E4038201050002820100 5B7C602A155775741EAAC552562B46D766D9917946D9C66E09
509BBB26E6A05EA5E45B95A797ED59E7BA6F06E15B3355A472DF734D625F4BFD41D9F3FF52F48D0E
D17285E70EF203D4EB97C915D5AEF2EE32F3F00BC742D080E7635AB49EF3624F6AB27E3270E082B8
C7FD5E0610259993D931719F5D6A8165A62E209A1734242C5E161AC68B5670F8CA58BF7C6ED25E79
812DAE633EB94C5A9E9614777FB7038A200965266E46145173C8EA9EB91C35550A335F6E7E4C1FBD
2D43E67CC7422E3D4D6AE931A4AD817335600BD76642196568013BDCC98973E57EE281004BEC7539
8559E27FE893A6F3BC1E11ACDB1DB4453343B0219A8C6D15AB280EFFB05F37
```

Enable the SSH server function.

```
[SwitchB] ssh server enable
```

Set the authentication mode for the user interface to AAA, and enable the user interface to support SSH.

```
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
[SwitchB-ui-vty0-15] protocol inbound ssh
[SwitchB-ui-vty0-15] quit
```

Create a local user **client001**.

```
[SwitchB] local-user client001
New local user added.
[SwitchB-luser-client001] password simple aabbcc
[SwitchB-luser-client001] service-type ssh
[SwitchB-luser-client001] authorization-attribute level 3
[SwitchB-luser-client001] quit
```

Specify the service type for the user **client001** as **Stelnet** and the authentication method as **password**.

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

Configuring Switch A

Assign an IP address to VLAN interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.105 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] quit
```

If first-time authentication is enabled, the configuration on Switch A is completed, and you can establish a connection with the server from the client.

If first-time authentication is disabled, proceed with the following configurations:

Enter public key view.

```
[SwitchA] public-key peer key1
Public key view: return to System View with "peer-public-key end".
```

Enter public key code view.

```
[SwitchA-pkey-public-key] public-key-code begin
Public key code view: return to last view with "public-key-code end".
```

Enter the host public key of the SSH server. (You can get the server's host public key by using the **display public-key local dsa public** command on the server.)

```
[SwitchA-pkey-key-code]3082033B3082022E06072A8648CE380401308202210282010100F13ACC169
3AFD04B9E1E8D2A9DEA
[SwitchA-pkey-key-code]6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E6
768193914B823BDF215
[SwitchA-pkey-key-code]D0DAD7A151E434F9E128DAFB9DEFAE07874621E70D7FC4577D2851C707BC8
6AC0FD3829B862C5CD7
[SwitchA-pkey-key-code]003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74DA31D
A0415264F3FA3E1A6E0
[SwitchA-pkey-key-code]F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE794C09A6C7DD
E05F1E0E928E82EEA31
[SwitchA-pkey-key-code]DB2454CD2E6866599DDF2381163734AD5C6F8A98A791BAD8942A5D12D674F
CA42EA93FF7FDD23E4E
[SwitchA-pkey-key-code]E29C35F75C8E52EF1B132073679EE2E62DF435CE35BB7F0FB756DF92A95C3
652F979BD03F8D2BB62
[SwitchA-pkey-key-code]018B021500C773218C737EC8EE993B4F2DED30F48EDACE915F0282010100D
43E90A700F70A4EE08C
[SwitchA-pkey-key-code]728A297DA04566A0A112DC49ABF51A37BBB56BFE518BBDCD71359EACE9871
2BEC58A261FC6D5FE78
[SwitchA-pkey-key-code]B9A67ED494288CB5A1984CA67037A16BFC75B889829C92465BA094460D7EE
F918969C0ADAE4841D1
[SwitchA-pkey-key-code]4A880142151C394C28F2731304C456350479D62014C81F07A0BA5FD0F9301
D8F9AF9F30C6D21471F
[SwitchA-pkey-key-code]00B65714991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBC
E7D283D144D4F5B5B61
[SwitchA-pkey-key-code]B4ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA
36E3DAE08B774836A3B
[SwitchA-pkey-key-code]5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B4
30B003ACDEB6C9B213A
[SwitchA-pkey-key-code]8749765992E4038201050002820100 5B7C602A155775741EAAC552562B46D
766D9917946D9C66E09
[SwitchA-pkey-key-code]509BBB26E6A05EA5E45B95A797ED59E7BA6F06E15B3355A472DF734D625F4
BFD41D9F3FF52F48D0E
[SwitchA-pkey-key-code]D17285E70EF203D4EB97C915D5AEF2EE32F3F00BC742D080E7635AB49EF36
24F6AB27E3270E082B8
[SwitchA-pkey-key-code]C7FD5E0610259993D931719F5D6A8165A62E209A1734242C5E161AC68B567
0F8CA58BF7C6ED25E79
```

```
[SwitchA-pkey-key-code]812DAE633EB94C5A9E9614777FB7038A200965266E46145173C8EA9EB91C3
5550A335F6E7E4C1FBD
[SwitchA-pkey-key-code]2D43E67CC7422E3D4D6AE931A4AD817335600BD76642196568013BDCC9897
3E57EE281004BEC7539
[SwitchA-pkey-key-code]8559E27FE893A6F3BC1E11ACDB1DB4453343B0219A8C6D15AB280EFFB05F3
7
```

Return to public key view and save the host public key.

```
[SwitchA-pkey-key-code] public-key-code end
```

Return to system view.

```
[SwitchA-pkey-public-key] peer-public-key end
```

Specify the host public key name of the Stelnet server (192.168.0.51) as **key1**.

```
[SwitchA] ssh client authentication server 192.168.0.51 assign publickey key1
[SwitchA] quit
```

Verifying the configuration

- If first-time authentication is enabled, verify the following items:
  - The client can authenticate the server and save the server's host public key locally.
  - You can log in to Switch B after entering the correct password.

```
<SwitchA> ssh 192.168.0.51
Username: client001
Trying 192.168.0.51 ...
Press CTRL+K to abort
Connected to 192.168.0.51 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:

***************************************************************************
* Copyright (c) 2004-2013 Hewlett-Packard Development Company,L.P.        *
* Without the owner's prior written consent,                              *
* no decompiling or reverse-engineering shall be allowed.                 *
***************************************************************************

<SwitchB>
```

- If first-time authentication is disabled, verify that you can log in to Switch B after entering the correct password.

```
<SwitchA> ssh2 192.168.0.51
Username: client001
Trying 192.168.0.51
Press CTRL+K to abort
Connected to 192.168.0.51...
Enter password:
***************************************************************************
* Copyright (c) 2004-2013 Hewlett-Packard Development Company,L.P.        *
```

```
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<SwitchB>
```

Configuration files

- Switch A:

```
#
vlan 1
#
 public-key peer key1
  public-key-code begin
   3082033B3082022E06072A8648CE380401308202210282010100F13ACC1693AFD04B9E1E8D
   2A9DEA6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E67681939
   14B823BDF215D0DAD7A151E434F9E128DAFB9DEFAE07874621E70D7FC4577D2851C707BC86
   AC0FD3829B862C5CD7003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74
   DA31DA0415264F3FA3E1A6E0F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE7
   94C09A6C7DDE05F1E0E928E82EEA31DB2454CD2E6866599DDF2381163734AD5C6F8A98A791
   BAD8942A5D12D674FCA42EA93FF7FDD23E4EE29C35F75C8E52EF1B132073679EE2E62DF435
   CE35BB7F0FB756DF92A95C3652F979BD03F8D2BB62018B021500C773218C737EC8EE993B4F
   2DED30F48EDACE915F0282010100D43E90A700F70A4EE08C728A297DA04566A0A112DC49AB
   F51A37BBB56BFE518BBDCD71359EACE98712BEC58A261FC6D5FE78B9A67ED494288CB5A198
   4CA67037A16BFC75B889829C92465BA094460D7EEF918969C0ADAE4841D14A880142151C39
   4C28F2731304C456350479D62014C81F07A0BA5FD0F9301D8F9AF9F30C6D21471F00B65714
   991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBCE7D283D144D4F5B5B61B4
   ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA36E3DAE08B77483
   6A3B5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B430B003ACD
   EB6C9B213A8749765992E4038201050002820100 5B7C602A155775741EAAC552562B46D766
   D9917946D9C66E09509BBB26E6A05EA5E45B95A797ED59E7BA6F06E15B3355A472DF734D62
   5F4BFD41D9F3FF52F48D0ED17285E70EF203D4EB97C915D5AEF2EE32F3F00BC742D080E763
   5AB49EF3624F6AB27E3270E082B8C7FD5E0610259993D931719F5D6A8165A62E209A173424
   2C5E161AC68B5670F8CA58BF7C6ED25E79812DAE633EB94C5A9E9614777FB7038A20096526
   6E46145173C8EA9EB91C35550A335F6E7E4C1FBD2D43E67CC7422E3D4D6AE931A4AD817335
   600BD76642196568013BDCC98973E57EE281004BEC75398559E27FE893A6F3BC1E11ACDB1D
   B4453343B0219A8C6D15AB280EFFB05F37
  public-key-code end
 peer-public-key end
#
interface Vlan-interface1
 ip address 192.168.0.105 255.255.255.0
#
 ssh client authentication server 192.168.0.51 assign publickey key1
#
```

- Switch B:

```
#
vlan 1
```

```
#
local-user client001
 password cipher $c$3$G+xmuBmDrurppAOsyNcYNzNqB+C/NSFsPg==
 authorization-attribute level 3
 service-type ssh
#
interface Vlan-interface1
 ip address 192.168.0.51 255.255.255.0
#
 ssh server enable
 ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 15
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
#
```

Example: Configuring the switch as an SFTP client for publickey authentication

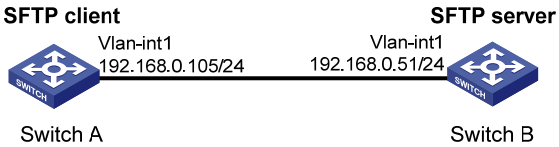
Applicable product matrix

Product series	Software version
HP 7500	Release 6620 Release 6630 Release 6700

Network requirements

As shown in Figure 220, you can log in to Switch B through the SFTP client that runs on Switch A for file management and transfer. Switch B acts as the SFTP server and uses publickey authentication and DSA public key algorithm.

Figure 220 Network diagram



Requirements analysis

For successful publickey authentication, do the following:

- Generate a DSA key pair on Switch A.
- Upload the switch's host public key to Switch B.
- Specify the host public key of Switch A for the SSH user on Switch B.

To enable Switch A to authenticate Switch B, you must also generate a DSA key pair on Switch B.

Configuration procedures

Configuring Switch A as an SFTP client

Assign an IP address to VLAN interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.105 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Generate a DSA key pair.

```
[SwitchA] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++.++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
```

Export the DSA host public key to the file **key2.pub**.

```
[SwitchA] public-key local export dsa ssh2 key2.pub
..
[SwitchA] quit
```

Configuring Switch B as an FTP server

Assign an IP address to VLAN interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.51 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Create a local user. The service type is **ftp** and the username and password are both **ftp**.

```
[SwitchB] local-user ftp
New local user added.
[SwitchB-luser-ftp] password simple ftp
[SwitchB-luser-ftp] authorization-attribute level 3
```

```
[SwitchB-luser-ftp] authorization-attribute work-directory flash:/
[SwitchB-luser-ftp] service-type ftp
[SwitchB-luser-ftp] quit
```

Enable the FTP server function on Switch B.

```
[SwitchB] ftp server enable
[SwitchB] quit
```

Uploading the public key file to the server

Log in to the FTP server from Switch A, and upload the public key file to the server.

```
<SwitchA> ftp 192.168.0.51
Trying 192.168.0.51 ...
Press CTRL+K to abort
Connected to 192.168.0.51.
220 FTP service ready.
User(192.168.0.51:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]put key2.pub
227 Entering Passive Mode (192,168,0,51,8,157).
125 ASCII mode data connection already open, transfer starting for /key2.pub.
226 Transfer complete.
FTP: 1187 byte(s) sent in 0.206 second(s), 5.00Kbyte(s)/sec.

[ftp] quit
```

Configuring Switch B as the SFTP server

1. Generate a DSA public key pair.

```
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++
```

2. Enable the SSH server function.

```
[SwitchB] ssh server enable
```

3. Enable the SFTP server.

```
[SwitchB] sftp server enable
```

4. Configure the VTY user interfaces:

Enable scheme authentication.

```
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
```

Enable the user interface to support SSH in the inbound direction.

```
[SwitchB-ui-vty0-15] protocol inbound ssh
```

Set the user privilege level to 3.

```
[SwitchB-ui-vty0-15] user privilege level 3
[SwitchB-ui-vty0-15] quit
```

5. Import the peer public key from the file **key2.pub**.

```
[SwitchB] public-key peer Switch001 import sshkey key2.pub
```

6. Configure a local user account for the SSH user:

Create a local user account named **client002**.

```
[SwitchB] local-user client002
New local user added.
```

Specify the service type as **SSH**.

```
[SwitchB-luser-client002] service-type ssh
```

Set the user privilege level to **3**.

```
[SwitchB-luser-client002] authorization-attribute level 3
[SwitchB-luser-client002] quit
```

7. Configure the SSH user:
   - Specify the service type as **sftp** and authentication method as **publickey** for the user **client002**.
   - Assign the public key **Switch001** to the user.
   - Specify the working directory as **flash:/**.

```
[SwitchB] ssh user client002 service-type sftp authentication-type publickey assign
publickey Switch001 work-directory flash:/
```

Verifying the configuration

To verify that the SFTP client is configured correctly for publickey authentication:

Establish a connection to the SFTP server and enter SFTP client view.

```
<SwitchA> sftp 192.168.0.51 identity-key dsa
Input Username: client002
Trying 192.168.0.51 ...
Press CTRL+K to abort
Connected to 192.168.0.51 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n

sftp-client>
```

Display files under the current directory of the server.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      5268 Apr 26 23:50 startup.cfg
-rwxrwxrwx   1 noone    nogroup  13138750 Apr 26 13:52 switchB.bin
drwxrwxrwx   1 noone    nogroup         0 Apr 26 12:00 seclog
-rwxrwxrwx   1 noone    nogroup    466612 Apr 26 14:25 switchB.btm
-rwxrwxrwx   1 noone    nogroup       287 Apr 26 23:50 system.xml
-rwxrwxrwx   1 noone    nogroup      1187 Apr 26 15:06 key2.pub
sftp-client>
```

Add a directory named **new1** and verify the result.

```
sftp-client> mkdir new1
New directory created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      5268 Apr 26 23:50 startup.cfg
-rwxrwxrwx   1 noone    nogroup  13138750 Apr 26 13:52 switchB.bin
drwxrwxrwx   1 noone    nogroup         0 Apr 26 12:00 seclog
-rwxrwxrwx   1 noone    nogroup    466612 Apr 26 14:25 switchB.btm
-rwxrwxrwx   1 noone    nogroup       287 Apr 26 23:50 system.xml
-rwxrwxrwx   1 noone    nogroup      1187 Apr 26 15:06 key2.pub
drwxrwxrwx   1 noone    nogroup         0 Apr 26 15:16 new1
```

Rename directory **new1** to **new2** and verify the result.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      5268 Apr 26 23:50 startup.cfg
-rwxrwxrwx   1 noone    nogroup  13138750 Apr 26 13:52 switchB.bin
drwxrwxrwx   1 noone    nogroup         0 Apr 26 12:00 seclog
-rwxrwxrwx   1 noone    nogroup    466612 Apr 26 14:25 switchB.btm
-rwxrwxrwx   1 noone    nogroup       287 Apr 26 23:50 system.xml
-rwxrwxrwx   1 noone    nogroup      1187 Apr 26 15:06 key2.pub
drwxrwxrwx   1 noone    nogroup         0 Apr 26 15:16 new2
```

Exit SFTP client view.

```
sftp-client> quit
Bye
Connection closed.
<SwitchA>
```

Configuration files

- Switch A:

```
#
vlan 1
#
 public-key peer Switch001
  public-key-code begin
   3082033B3082022E06072A8648CE380401308202210282010100F13ACC1693AFD04B9E1E8D
   2A9DEA6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E67681939
   14B823BDF215D0DAD7A151E434F9E128DAFB9DEFAE07874621E70D7FC4577D2851C707BC86
   AC0FD3829B862C5CD7003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74
   DA31DA0415264F3FA3E1A6E0F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE7
   94C09A6C7DDE05F1E0E928E82EEA31DB2454CD2E6866599DDF2381163734AD5C6F8A98A791
   BAD8942A5D12D674FCA42EA93FF7FDD23E4EE29C35F75C8E52EF1B132073679EE2E62DF435
   CE35BB7F0FB756DF92A95C3652F979BD03F8D2BB62018B021500C773218C737EC8EE993B4F
   2DED30F48EDACE915F0282010100D43E90A700F70A4EE08C728A297DA04566A0A112DC49AB
   F51A37BBB56BFE518BBDCD71359EACE98712BEC58A261FC6D5FE78B9A67ED494288CB5A198
   4CA67037A16BFC75B889829C92465BA094460D7EEF918969C0ADAE4841D14A880142151C39
```

```
   4C28F2731304C456350479D62014C81F07A0BA5FD0F9301D8F9AF9F30C6D21471F00B65714
   991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBCE7D283D144D4F5B5B61B4
   ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA36E3DAE08B77483
   6A3B5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B430B003ACD
   EB6C9B213A8749765992E40382010500028201001CBCFC26EBDF618121FA5B4934E0A591EC
   B11954AE88AE577A87866D2861B1DB8629B65BE2E2892455EF125A936528338375BF0CEA85
   F502FA2D0AA22675AE7908D06F34334FFE550B3D30EC28ABB668B0CAC9F8D26A198F4C8A0A
   DC086E9F8A30E8F8035B3949F6004F18A6DA21E7A1DBAE52F56ABFD5B9A32A52C6F43A272C
   9CAA7C751F0711BCECBE86BB16F0FC3939BD262B8732C6859156C456C01989EB37A275E8C9
   D4A2091433205693760557E3CA8A3CDA432856026C2F6279CC516CA84265CA63621DFB97A7
   2A40BC3C6DAD3A7D6DEDD3550293A81A36767C41501E7ECB217C85EC3779CAF0514C479A8D
   D476C2D4D1BE2A9D29F0206006CED45675
  public-key-code end
 peer-public-key end
#
interface Vlan-interface1
 ip address 192.168.0.105 255.255.255.0
#
 ssh user client002 service-type sftp authentication-type publickey
assign publickey Switch001
```

- Switch B:

```
#
 ftp server enable
#
vlan 1
#
local-user client002
 authorization-attribute level 3
 service-type ssh
#
local-user ftp
 password cipher $c$3$1KhhVXwJ6k3Ms0RMDqHOYCEKHzhULw==
 authorization-attribute work-directory flash:/
 authorization-attribute level 3
 service-type ftp
#
interface Vlan-interface1
 ip address 192.168.0.51 255.255.255.0
#
user-interface vty 0 15
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
#
```

Static multicast route configuration examples

This chapter provides static multicast route configuration examples.

Static multicast routes are used only for RFP check. They are not used for multicast data forwarding.

General configuration restrictions and guidelines

When you specify an RPF neighbor in a static multicast route, specify its IP address instead of the interface connected to it.

Example: Configuring static multicast routes (for changing RPF routes)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

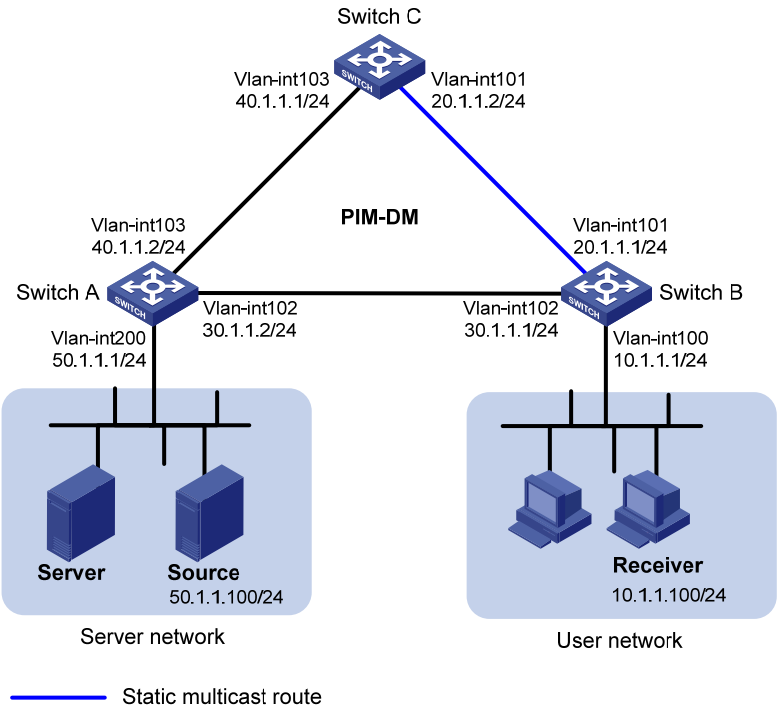
Network requirements

As shown in Figure 221:

- The server network and user network access the PIM-DM network through Switch A and Switch B.
- The server network sends large amounts of unicast packets and multicast packets to the user network.

Configure a static multicast route on switch B for multicast traffic to travel along a different path than unicast traffic. This configuration optimizes load distribution in the network.

Figure 221 Network diagram



Requirements analysis

Before you configure a static multicast route, do the following:

- Display RPF neighbor information on Switch B.
- Examine which RPF neighbor is used by the unicast route to the multicast source.

Then, configure a static multicast route to the multicast source with a different RPF neighbor than that of the unicast route.

Configuration procedures

1. Configure the IP address and subnet mask for each interface, as shown in Figure 221. (Details not shown.)
2. Enable OSPF on the switches in the PIM-DM domain to make sure both of the following conditions exist (details not shown):
   - The network layer on the PIM-DM network is interoperable.
   - The routing information among the switches can be dynamically updated.
3. Configure multicast on Switch A and Switch C:

   # Enable IP multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing-enable
   ```

   # Enable PIM-DM on each interface.

   ```
   [SwitchA] interface vlan-interface 200
   [SwitchA-Vlan-interface200] pim dm
   ```

```
[SwitchA-Vlan-interface200] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```

Enable IP multicast routing and PIM-DM on Switch C in the same way Switch A is configured.

4. Configure multicast on Switch B:

Enable IP multicast routing globally.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
```

Enable IGMP on VLAN interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
```

Enable PIM-DM on each interface.

```
[SwitchB-Vlan-interface100] pim dm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim dm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim dm
```

Display the RPF route to the source.

```
[SwitchB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2
     Referenced route/mask: 50.1.1.0/24
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

The output shows the following:

- The current RPF route on Switch B is contributed by a unicast routing protocol.
- The RPF neighbor is Switch A.

Configure a static multicast route, specifying Switch C as its RPF neighbor on the route to the source.

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

Verifying the configuration

To verify that the RPF route is changed by the static multicast route, use the **display multicast rpf-info** command on Switch B to display information about the RPF route to the source.

```
[SwitchB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2
     Referenced route/mask: 50.1.1.0/24
```

```
    Referenced route type: multicast static
    Route selection rule: preference-preferred
    Load splitting rule: disable
```

The output shows the following:

- The RPF route to the source on Switch B is the configured static multicast route.
- The RPF neighbor of Switch B is Switch C.

Complete configuration

- Switch A:

```
#
 multicast routing-enable
#
vlan 102 to 103
#
vlan 200
#
interface Vlan-interface102
 ip address 30.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface103
 ip address 40.1.1.2 255.255.255.0
 pim dm
#
interface Vlan-interface200
 ip address 50.1.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  network 50.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
 multicast routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0.
 igmp enable
 pim dm
#
interface Vlan-interface101
```

```
 ip address 20.1.1.1 255.255.255.0.
 pim dm
#
interface Vlan-interface102
 ip address 30.1.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
ip rpf-route-static 50.1.1.0 24 20.1.1.2
#
```

- Switch C:

```
#
 multicast routing-enable
#
vlan 101
#
vlan 103
#
interface Vlan-interface101
 ip address 20.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface103
 ip address 40.1.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
#
```

Example: Configuring static multicast routes (for creating RPF routes)

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

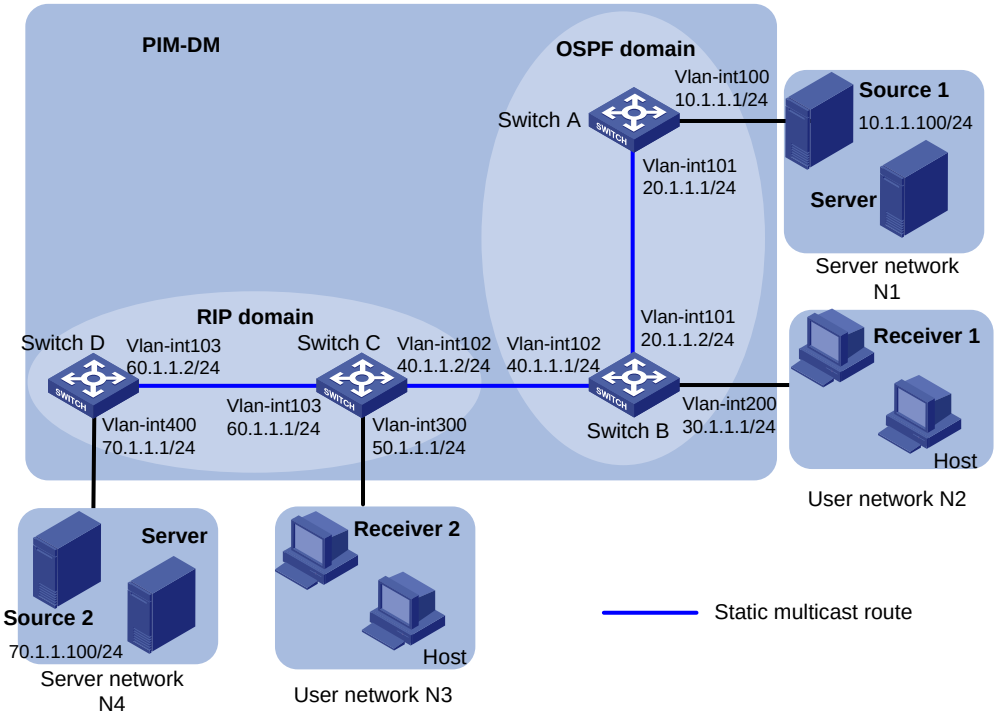
Network requirements

As shown in Figure 222:

- The PIM-DM network is divided into an OSPF domain and a RIP domain for security purposes.
- The switches in each domain are interoperable at the network layer.
- The unicast routes between the OSPF domain and the RIP domain are isolated and not redistributed.
- The server network N1 and user network N2 access the OSPF domain. The server network N4 and user network N3 access the RIP domain.
- Receiver 1 and Receiver 2 can receive multicast packets from Source 1 and Source 2, respectively.

Configure static multicast routes so that the OSPF domain and RIP domain are interoperable in multicast transmission but isolated in unicast data transmission. As a result, Receiver 1 and Receiver 2 can receive multicast packets from both Source 1 and Source 2.

Figure 222 Network diagram



Requirements analysis

To meet the network requirements, configure static multicast routes on the following devices:

- Devices that are located between the receivers and the multicast source.
- Devices that do not have unicast routes to the multicast source.

Configuration procedures

1. Configure the IP address and subnet mask for each interface, as shown in Figure 222. (Details not shown.)
2. Configure OSPF on Switch A and Switch B. (Details not shown.)
3. Configure RIP on Switch C and Switch D. (Details not shown.)
4. Enable IP multicast routing, IGMP, and PIM-DM:
   - On Switch A:

     # Enable IP multicast routing globally.

     ```
     <SwitchA> system-view
     [SwitchA] multicast routing-enable
     ```

     # Enable PIM-DM on each interface.

     ```
     [SwitchA] interface vlan-interface 100
     [SwitchA -Vlan-interface100] pim dm
     [SwitchA -Vlan-interface100] quit
     [SwitchA] interface vlan-interface 101
     [SwitchA-Vlan-interface101] pim dm
     [SwitchA-Vlan-interface101] quit
     ```

- Enable IP multicast routing and PIM-DM on Switch D in the same way Switch A is configured. (Details not shown.)
- On Switch B:

  # Enable IP multicast routing globally.

  ```
  <SwitchB> system-view
  [SwitchB] multicast routing-enable
  ```

  # Enable IGMP on VLAN interface 200.

  ```
  [SwitchB] interface vlan-interface 200
  [SwitchB-Vlan-interface200] igmp enable
  ```

  # Enable PIM-DM on each interface.

  ```
  [SwitchB-Vlan-interface200] pim dm
  [SwitchB-Vlan-interface200] quit
  [SwitchB] interface vlan-interface 101
  [SwitchB-Vlan-interface101] pim dm
  [SwitchB-Vlan-interface101] quit
  [SwitchB] interface vlan-interface 102
  [SwitchB-Vlan-interface102] pim dm
  [SwitchB-Vlan-interface102] quit
  ```

- Enable IP multicast routing, IGMP, and PIM-DM on Switch C in the same way Switch B is configured. (Details not shown.)

5. Display information about the RPF route to Source 2 on Switch B.

   ```
   [SwitchB] display multicast rpf-info 70.1.1.100
   ```

   No output is displayed, which means that no RPF routes to Source 2 exist on Switch B.

   Execute the same command on Switch C. No output is displayed for Switch C, either, which means that no RPF routes to Source 1 exist on Switch C.

6. Configure static multicast routes:

   # Configure a static multicast route on Switch B, specifying Switch C as its RPF neighbor on the route to Source 2.

   ```
   [SwitchB] ip rpf-route-static 70.1.1.100 24 40.1.1.2
   ```

   # Configure a static multicast route on Switch C, specifying Switch B as its RPF neighbor on the route to the source 1.

   ```
   [SwitchC] ip rpf-route-static 10.1.1.100 24 40.1.1.1
   ```

Verifying the configuration

To verity that RPF routes are created based on the static multicast routes:

Use the **display multicast rpf-info** command on Switch B to display information about the RPF route to Source 2.

```
[SwitchB] display multicast rpf-info 70.1.1.100
 RPF information about source 70.1.1.100:
     RPF interface: Vlan-interface102, RPF neighbor: 40.1.1.2
     Referenced route/mask: 70.1.1.0/24
     Referenced route type: multicast static
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Use the **display multicast rpf-info** command on Switch C to display information about the RPF route to Source 1.

```
[SwitchC] display multicast rpf-info 10.1.1.100
 RPF information about source 10.1.1.100:
     RPF interface: Vlan-interface101, RPF neighbor: 40.1.1.1
     Referenced route/mask: 10.1.1.0/24
     Referenced route type: multicast static
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

The output shows the following:

- The RPF routes to Source 2 and Source 1 are available on Switch B and Switch C, respectively.
- The RPF are the configured static routes.

Configuration files

- Switch A:

```
#
 multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0.
 pim dm
#
interface Vlan-interface101
 ip address 20.1.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
 multicast routing-enable
#
vlan 101 to 102
#
vlan 200
#
interface Vlan-interface101
 ip address 20.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface102
```

```
 ip address 40.1.1.1 255.255.255.0.
 pim dm
#
interface Vlan-interface200
 ip address 30.1.1.1 255.255.255.0
 igmp enable
 pim dm
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
ip rpf-route-static 70.1.1.0 24 40.1.1.2
#
```

- Switch C:

```
#
 multicast routing-enable
#
vlan 102 to 103
#
vlan 300
#
interface Vlan-interface102
 ip address 40.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface103
 ip address 60.1.1.1 255.255.255.0.
 pim dm
#
interface Vlan-interface300
 ip address 50.1.1.1 255.255.255.0
 igmp enable
 pim dm
#
rip 1
 network 50.0.0.0
 network 60.0.0.0
#
ip rpf-route-static 10.1.1.0 24 40.1.1.1
#
```

- Switch D:

```
#
 multicast routing-enable
#
vlan 103
#
```

```
vlan 400
#
interface Vlan-interface103
 ip address 60.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface400
 ip address 70.1.1.1 255.255.255.0
 pim dm
#
rip 1
 network 60.0.0.0
 network 70.0.0.0
#
```

Example: Configure multicast forwarding over a GRE tunnel

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

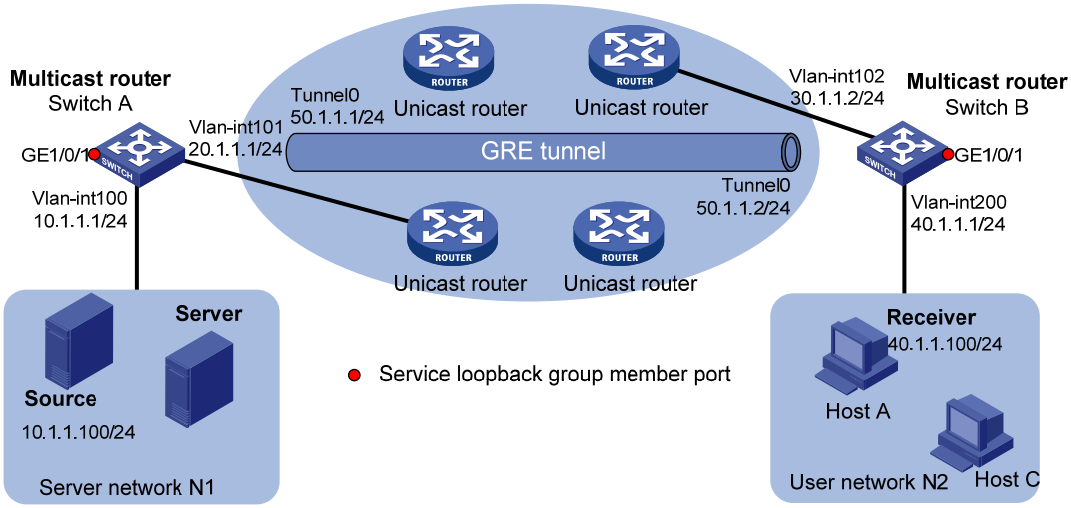
Network requirements

As shown in Figure 223:

- The server networks N1 and N2 access the intermediate network through Switch A and Switch B, respectively.
- The routers in the intermediate network do not support multicast. Switch A and Switch B support multicast and run PIM-DM.
- All routers and switches are interoperable through unicast routes.

Configure multicast forwarding over a GRE tunnel between Switch A and Switch B, so that Host A in N2 can receive multicast packets from the source in N1.

Figure 223 Network diagram



Requirements analysis

Do not configure static unicast route at both ends of the tunnel. Configure a static multicast route toward the multicast source at the receiver end of the tunnel, specifying the RPF neighbor as the IP address of the source end of the tunnel.

Configuration restrictions and guidelines

When you configure multicast forwarding over a GRE tunnel, follow these restrictions and guidelines:

- Before the configuration, make sure the devices at the two ends of the tunnel are interoperable through unicast route.
- The source address and destination address of a tunnel uniquely identify a path. You must specify the source address and destination address for a tunnel at one end, and reverse the setting at the other end.
- Before you configure a GRE tunnel, do the following:
  - Create a service loopback group.
  - Specify its service type as **Tunnel**.
  - Add an unused Layer 2 Ethernet port to the service loopback group.

Configuration procedures

1. Configure the IP address and subnet mask for each interface, as shown in Figure 223. (Details not shown.)

   Configure OSPF on the switches. (Details not shown.)
2. Configure a GRE tunnel:
   - On Switch A:
     # Create interface Tunnel 0, and assign an IP address to this interface.

     ```
     <SwitchA> system-view
     [SwitchA] interface tunnel 0
     ```

```
[SwitchA-Tunnel0] ip address 50.1.1.1 24
```

Specify the tunnel encapsulation mode as GRE, and specify its source and destination addresses.

```
[SwitchA-Tunnel0] tunnel-protocol gre
[SwitchA-Tunnel0] source 20.1.1.1
[SwitchA-Tunnel0] destination 30.1.1.2
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **Tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Disable STP and LLDP on interface GigabitEthernet 1/0/1.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] undo stp enable
[SwitchA-GigabitEthernet1/0/1] undo lldp enable
```

Add GigabitEthernet 1/0/1 to service loopback group 1. GigabitEthernet 1/0/1 is idle and does not belong to VLAN 100 or VLAN 101.

```
[SwitchA-GigabitEthernet1/0/1] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/1] quit
```

In tunnel interface view, reference the service loopback group 1 on tunnel 0.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

- On Switch B:

Create interface Tunnel 0, and assign an IP address to this interface.

```
<SwitchB> system-view
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ip address 50.1.1.2 24
```

Specify the tunnel encapsulation mode as GRE over IPv4, and specify its source and destination addresses.

```
[SwitchB-Tunnel0] tunnel-protocol gre
[SwitchB-Tunnel0] source 30.1.1.2
[SwitchB-Tunnel0] destination 20.1.1.1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as Tunnel.

```
[SwitchB] service-loopback group 1 type tunnel
```

Disable STP and LLDP on interface GigabitEthernet 1/0/1.

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] undo stp enable
[SwitchB-GigabitEthernet1/0/1] undo lldp enable
```

Add GigabitEthernet 1/0/1 to service loopback group 1. GigabitEthernet 1/0/1 is idle and does not belong to VLAN 102 or VLAN 200.

```
[SwitchB-GigabitEthernet1/0/1] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/1] quit
```

In tunnel interface view, reference the service loopback group 1 on tunnel 0.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
```

```
[SwitchB-Tunnel0] quit
```

3. Configure OSPF:

   # Configure OSPF on 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 20.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

   # Configure OSPF on Switch B.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

4. Enable IP multicast routing, PIM-DM, and IGMP:

   - On Switch A:

     # Enable multicast routing globally.

```
[SwitchA] multicast routing-enable
```

     # Enable PIM-DM on the interfaces through which the multicast data passes.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] pim dm
[SwitchA-Tunnel0] quit
```

   - On Switch B:

     # Enable multicast routing globally.

```
[SwitchB] multicast routing-enable
```

     # Enable IGMP on VLAN-interface 200

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
```

     # Enable PIM-DM on the interfaces through which the multicast data passes.

```
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] pim dm
[SwitchB-Tunnel0] quit
```

5. On Switch B, configure a static multicast route, specifying the RPF neighbor toward the source as interface Tunnel 0 on Switch A.

```
[SwitchB] ip rpf-route-static 10.1.1.0 24 50.1.1.1
```

Verifying the configuration

To verify that multicast forwarding over the GRE tunnel is configured correctly:

1. Send multicast data from the source to the multicast group 225.1.1.1.
2. Verify that Host A can receive the multicast data after joining the multicast group.
3. Display PIM routing table information on Switch B.

```
[SwitchB] 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: 00:04:25
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface200
             Protocol: igmp, UpTime: 00:04:25, Expires: never

 (10.1.1.100, 225.1.1.1)
     Protocol: pim-dm, Flag:
     UpTime: 00:06:14
     Upstream interface: Tunnel0
         Upstream neighbor: 50.1.1.1
         RPF prime neighbor: 50.1.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface200
             Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

The output shows the following:

- Switch A is the RPF neighbor of Switch B.
- The multicast data from Switch A is delivered over a GRE tunnel to Switch B.

Configuration files

- Switch A:

```
#
 multicast routing-enable
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
```

```
 ip address 10.1.1.1 255.255.255.0
 pim dm
#
interface Vlan-interface101
 ip address 20.1.1.1 255.255.255.0
 pim dm
#
interface GigabitEthernet1/0/1
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ip address 50.1.1.1 255.255.255.0
 source 20.1.1.1
 destination 30.1.1.2
 service-loopback-group 1
 pim dm
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
 multicast routing-enable
#
 service-loopback group 1 type tunnel
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ip address 30.1.1.2 255.255.255.0
 pim dm
#
interface Vlan-interface200
 ip address 40.1.1.1 255.255.255.0
 igmp enable
 pim dm
#
interface GigabitEthernet1/0/1
 stp disable
 undo lldp enable
 port service-loopback group 1
#
```

```
interface Tunnel0
 ip address 50.1.1.2 255.255.255.0
 source 30.1.1.2
 destination 20.1.1.1
 service-loopback-group 1
 pim dm
#
ospf 1
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
#
ip rpf-route-static 10.1.1.0 24 50.1.1.1
#
```

Static routing configuration examples

This chapter provides static routing configuration examples.

Example: Configuring basic static routing

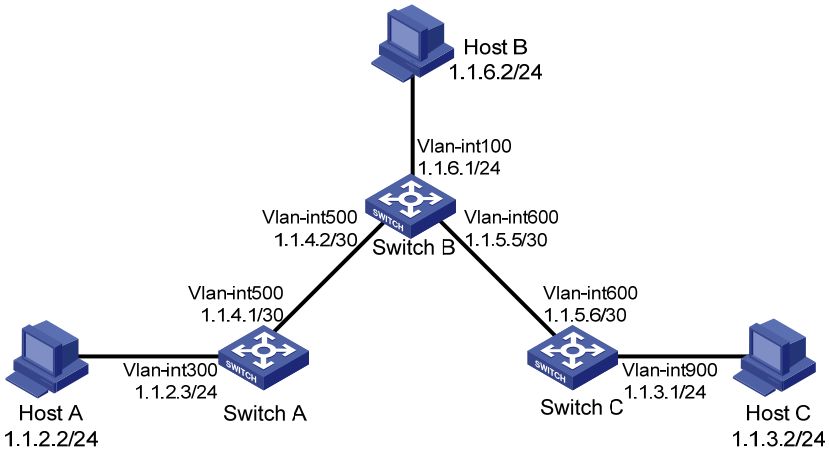
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 224, configure static routes on the switches for interconnections between any two hosts.

Figure 224 Network diagram



Configuration procedures

1. Configure the IP address for interfaces:

   # Configure IP addresses for interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 300
[SwitchA-Vlan300] interface Vlan-interface300
[SwitchA-Vlan-interface300] ip address 1.1.2.3 255.255.255.0
[SwitchA-Vlan-interface300] quit
[SwitchA] vlan 500
```

```
[SwitchA-Vlan500] interface Vlan-interface500
[SwitchA-Vlan-interface500] ip address 1.1.4.1 255.255.255.252
[SwitchA-Vlan-interface500] quit
```

Configure IP addresses for interfaces on Switch B.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-Vlan100] interface Vlan-interface100
[SwitchB-Vlan-interface100] ip address 1.1.6.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
[SwitchB] vlan 500
[SwitchB-Vlan500] interface Vlan-interface500
[SwitchB-Vlan-interface500] ip address 1.1.4.2 255.255.255.252
[SwitchB-Vlan-interface500] quit
[SwitchB] vlan 600
[SwitchB-Vlan600] interface Vlan-interface600
[SwitchB-Vlan-interface600] ip address 1.1.5.5 255.255.255.252
[SwitchB-Vlan-interface600] quit
```

Configure IP addresses for interfaces on Switch C.

```
<SwitchC> system-view
[SwitchC] vlan 600
[SwitchC-Vlan600] interface Vlan-interface600
[SwitchC-Vlan-interface600] ip address 1.1.5.6 255.255.255.252
[SwitchC-Vlan-interface600] quit
[SwitchC] vlan 900
[SwitchC-Vlan900] interface Vlan-interface900
[SwitchC-Vlan-interface900] ip address 1.1.3.1 255.255.255.0
[SwitchC-Vlan-interface900] quit
```

2. 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 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

Configure a default route on Switch C.

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

3. Configure the default gateways of Host A, Host B, and Host C as 1.1.2.3, 1.1.6.1, and 1.1.3.1, respectively. (Details not shown.)

Verifying the configuration

Use the **ping** command on the hosts to test the reachability. All hosts can reach one another.

Configuration files

- Switch A:

```
#
vlan 300
#
vlan 500
#
interface Vlan-interface300
 ip address 1.1.2.3 255.255.255.0
#
interface Vlan-interface500
 ip address 1.1.4.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
```

- Switch B:

```
#
vlan 100
#
vlan 500
#
vlan 600
#
interface Vlan-interface100
 ip address 1.1.6.1 255.255.255.0
#
interface Vlan-interface500
 ip address 1.1.4.2 255.255.255.252
#
interface Vlan-interface600
 ip address 1.1.5.5 255.255.255.252
#
 ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
 ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
#
```

- Switch C:

```
#
vlan 600
#
vlan 900
#
interface Vlan-interface600
 ip address 1.1.5.6 255.255.255.252
#
interface Vlan-interface900
 ip address 1.1.3.1 255.255.255.0
```

```
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
#
```

Example: Configuring static routing-Track-NQA collaboration

Applicable product matrix

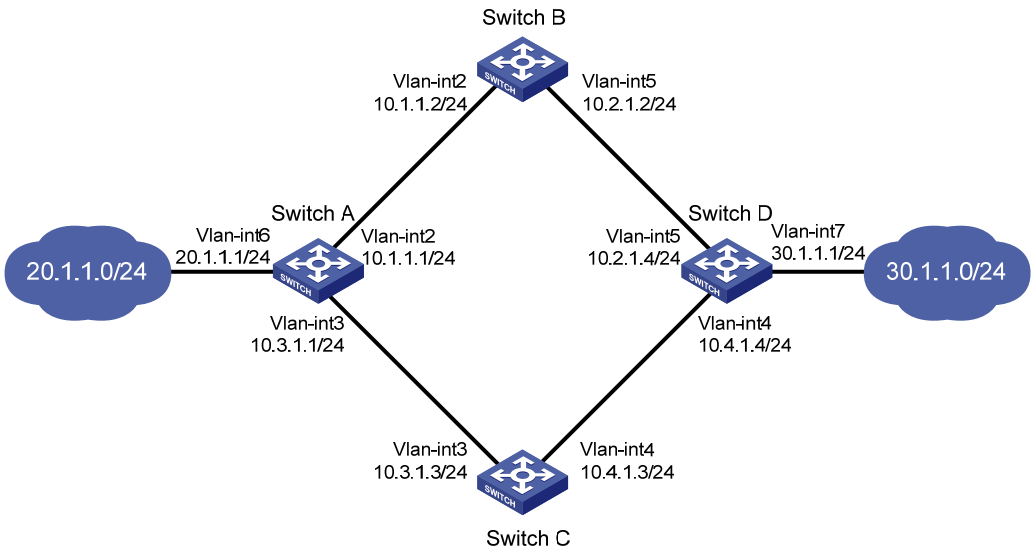
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 225, Switch A and Switch D are connected to two networks: 20.1.1.0/24 and 30.1.1.0/24.

Configure static routes on these switches so that the two networks can communicate with each other. Configure static routing-Track-NQA collaboration to enable quick link switchover when the primary route fails, improving network availability.

Figure 225 Network diagram



Configuration restrictions and guidelines

When you configure static routing-Track-NQA collaboration, follow these restrictions and guidelines:

- When you configure an ICMP-echo operation to test the connectivity of a path, you must specify the next hop to define the path.
- You cannot enter the operation view of a scheduled NQA operation. To modify the operation, first use the **undo nqa schedule** command to stop the operation.

Configuration procedures

1. Configure the IP address for interfaces, as shown in Figure 225. (Details not shown.)
2. Configure Switch A:

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.1.1.2 and the default priority 60. This static route is associated with track entry 1.

   ```
   <SwitchA> system-view
   [SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
   ```

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.3.1.3 and the priority 80.

   ```
   [SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
   ```

   # Configure a static route to 10.2.1.4, with the address of the next hop as 10.1.1.2.

   ```
   [SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
   ```

   # Create an NQA test group with the administrator **admin** and the operation tag **test**.

   ```
   [SwitchA] nqa entry admin test
   ```

   # Configure the test type as ICMP-echo.

   ```
   [SwitchA-nqa-admin-test] type icmp-echo
   ```

   # Configure the destination address of the test as 10.2.1.4 and the next hop address as 10.1.1.2 to check the connectivity of the path from Switch A to Switch B and then to Switch D through NQA.

   ```
   [SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
   [SwitchA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
   ```

   # Configure the test frequency as 100 milliseconds.

   ```
   [SwitchA-nqa-admin-test-icmp-echo] frequency 100
   ```

   # Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.

   ```
   [SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
   threshold-type consecutive 5 action-type trigger-only
   [SwitchA-nqa-admin-test-icmp-echo] quit
   ```

   # Start the NQA test.

   ```
   [SwitchA] nqa schedule admin test start-time now lifetime forever
   ```

   # Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the administrator **admin**, and the operation tag **test**).

   ```
   [SwitchA] track 1 nqa entry admin test reaction 1
   ```

3. Configure Switch B:

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.2.1.4.

   ```
   <SwitchB> system-view
   [SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
   ```

   # Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.1.1.1.

   ```
   [SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
   ```

4. Configure Switch C:

Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.4.1.4.

```
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.3.1.1.

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

5. Configure Switch D:

Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.2.1.2 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchD> system-view
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.4.1.3 and the priority 80.

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

Configure a static route to 10.1.1.1, with the address of the next hop as 10.2.1.2.

```
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
```

Create an NQA test group with the administrator **admin** and the operation tag **test**.

```
[SwitchD] nqa entry admin test
```

Configure the test type as ICMP-echo.

```
[SwitchD-nqa-admin-test] type icmp-echo
```

Configure the destination address of the test as 10.1.1.1 and the next hop address as 10.2.1.2 to check the connectivity of the path from Switch D to Switch B and then to Switch A through NQA.

```
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[SwitchD-nqa-admin-test-icmp-echo] next-hop 10.2.1.2
```

Configure the test frequency as 100 milliseconds.

```
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
```

Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.

```
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit
```

Start the NQA test.

```
[SwitchD] nqa schedule admin test start-time now lifetime forever
```

Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the administrator **admin**, and the operation tag **test**).

```
[SwitchD] track 1 nqa entry admin test reaction 1
```

Verifying the configuration

Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the NQA test result:

- The primary route is available (the status of the track entry is Positive).
- Switch A forwards packets to 30.1.1.0/24 through Switch B.

Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] shutdown
```

Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Negative
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public

         Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
```

The output shows the NQA test result:

- The primary route is unavailable (the status of the track entry is Negative).
- The backup static route takes effect; and Switch A forwards packets to 30.1.1.0/24 through Switch C.

When the primary route fails, the hosts in 20.1.1.0/24 can still communicate with the hosts in 30.1.1.0/24.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
  PING 30.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 30.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

The output on Switch D is similar to that on Switch A. When the primary route fails, the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24.

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
  PING 20.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 20.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Configuration files

- Switch A:

```
#
nqa entry admin test
 type icmp-echo
  destination ip 10.2.1.4
  frequency 100
  next-hop 10.1.1.2
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
 trigger-only
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
```

```
 ip route-static 30.1.1.0 255.255.255.0 10.1.1.2 track 1
 ip route-static 30.1.1.0 255.255.255.0 10.3.1.3 preference 80
#
 track 1 nqa entry admin test reaction 1
#
 nqa schedule admin test start-time now lifetime forever
#
```

- Switch B:

```
ip route-static 20.1.1.0 255.255.255.0 10.1.1.1
ip route-static 30.1.1.0 255.255.255.0 10.2.1.4
```

- Switch C:

```
ip route-static 20.1.1.0 255.255.255.0 10.3.1.1
ip route-static 30.1.1.0 255.255.255.0 10.4.1.4
```

- Switch D:

```
#
nqa entry admin test
 type icmp-echo
  destination ip 10.1.1.1
  frequency 100
  next-hop 10.2.1.2
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
 trigger-only
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.2
 ip route-static 20.1.1.0 255.255.255.0 10.2.1.2 track 1
 ip route-static 20.1.1.0 255.255.255.0 10.4.1.3 preference 80
#
 track 1 nqa entry admin test reaction 1
#
 nqa schedule admin test start-time now lifetime forever
#
```

Example: Configuring static routing-Track-BFD collaboration

Applicable product matrix

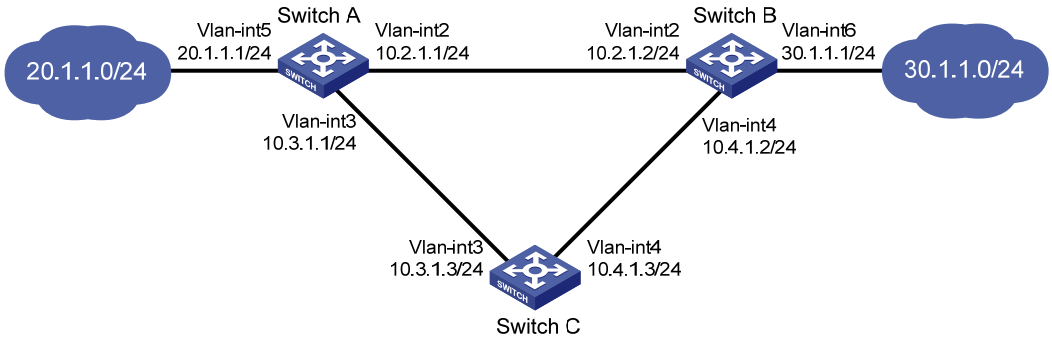
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 226, Switch A and Switch B are connected to two networks: 20.1.1.0/24 and 30.1.1.0/24.

Configure static routes on these switches so that the two networks can communicate with each other. Configure static routing-Track-BFD collaboration to enable quick link switchover when the primary route fails, improving network availability.

Figure 226 Network diagram



Configuration restrictions and guidelines

The source IP address of BFD echo packets cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Configuration procedures

1. Configure the IP address for interfaces, as shown in Figure 226. (Details not shown.)
2. Configure Switch A:

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.2.1.2 and the default priority 60. This static route is associated with track entry 1.

   ```
   <SwitchA> system-view
   [SwitchA] ip route-static 30.1.1.0 24 10.2.1.2 track 1
   ```

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.3.1.3 and the priority 80.

   ```
   [SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
   ```

   # Configure the source address of BFD echo packets as 10.10.10.10.

   ```
   [SwitchA] bfd echo-source-ip 10.10.10.10
   ```

   # Configure track entry 1, and associate it with the BFD session. Check whether Switch A can be interoperated with the next hop (Switch B) of the static route.

   ```
   [SwitchA] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip
   10.2.1.1
   ```

3. Configure Switch B:

   # Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.2.1.1 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchB> system-view
[SwitchB] ip route-static 20.1.1.0 24 10.2.1.1 track 1
```

Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.4.1.3 and the priority 80.

```
[SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

Configure the source address of BFD echo packets as 1.1.1.1.

```
[SwitchB] bfd echo-source-ip 1.1.1.1
```

Configure track entry 1 that is associated with the BFD session to check whether Switch B can communicate with the next hop (Switch A) of the static route.

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip
10.2.1.2
```

4. Configure Switch C:

Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.4.1.2.

```
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.2
```

Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.3.1.1.

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

Verifying the configuration

Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD Session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 10.2.1.2
    Local IP   : 10.2.1.1
```

Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 9        Routes : 9
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct 0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.2.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the BFD detection result:

- The next hop 10.2.1.2 is reachable (the status of the track entry is Positive).
- The primary static route takes effect; and Switch A forwards packets to 30.1.1.0/24 through Switch B.

Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] shutdown
```

Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Negative
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD Session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 10.2.1.2
    Local IP   : 10.2.1.1
```

Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 4        Routes : 4
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct 0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the BFD detection result:

- The next hop 10.2.1.2 is unreachable (the status of the track entry is Negative).
- The backup static route takes effect; and Switch A forwards packets to 30.1.1.0/24 through Switch C and Switch B.

When the primary route fails, the hosts in 20.1.1.0/24 can still communicate with the hosts in 30.1.1.0/24.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
  PING 30.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 30.1.1.1 ping statistics ---
```

```
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 ms
```

The output on Switch B is similar to that on Switch A. When the primary route fails, the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24.

```
[SwitchB] ping -a 30.1.1.1 20.1.1.1
  PING 20.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 20.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Configuration files

- Switch A:

```
#
bfd echo-source-ip 10.10.10.10
#
 ip route-static 30.1.1.0 24 10.2.1.2 track 1
 ip route-static 30.1.1.0 24 10.3.1.3 preference 80
#
 track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip 10.2.1.1
#
```

- Switch B:

```
#
bfd echo-source-ip 1.1.1.1
#
 ip route-static 30.1.1.0 24 10.2.1.2 track 1
 ip route-static 20.1.1.0 24 10.4.1.3 preference 80
#
track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip 10.2.1.2
#
```

- Switch C:

```
#
 ip route-static 20.1.1.0 24 10.3.1.1
 ip route-static 30.1.1.0 24 10.4.1.2
#
```

Tunnel configuration examples

This chapter provides tunnel configuration examples.

Example: Configuring an IPv6 over IPv4 manual tunnel

Applicable product matrix

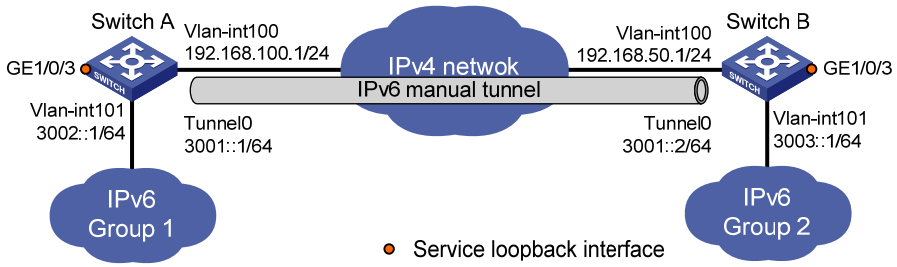
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 227, Switch A and Switch B can reach each other.

Configure an IPv6 over IPv4 manual tunnel between Switch A and Switch B so the two IPv6 networks can reach each other over the IPv4 network.

Figure 227 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 3002::1 64
[SwitchA-Vlan-interface101] quit
```

Configure an IPv6 over IPv4 manual tunnel.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] destination 192.168.50.1
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Configure a static route to IPv6 network Group 2 through the tunnel interface.

```
[SwitchA] ipv6 route-static 3003:: 64 tunnel 0
```

Configuring Switch B

Enable IPv6.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.168.50.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 3003::1 64
[SwitchB-Vlan-interface101] quit
```

Configure an IPv6 over IPv4 manual tunnel.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3001::2/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] destination 192.168.100.1
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

Configure a static route to IPv6 network Group 1 through the tunnel interface.

```
[SwitchB] ipv6 route-static 3002:: 64 tunnel 0
```

Verifying the configuration

Display the status of the tunnel interface on Switch A.

```
[SwitchA] display ipv6 interface tunnel 0 verbose
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::C0A8:6401
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF00:1
    FF02::1:FFA8:6401
    FF02::2
    FF02::1
  MTU is 1480 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                  55
…
```

Display the status of the tunnel interface on Switch B.

```
[SwitchB] display ipv6 interface tunnel 0 verbose
Tunnel0 current state :UP
```

```
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::C0A8:3201
  Global unicast address(es):
    3001::2, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF00:1
    FF02::1:FFA8:3201
    FF02::2
    FF02::1
  MTU is 1480 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   55
…
```

Ping the IPv6 address of the peer interface VLAN-interface 101 from Switch A. The ping operation succeeds.

```
[SwitchA] ping ipv6 3003::1
  PING 3003::1 : 56  data bytes, press CTRL_C to break
    Reply from 3003::1
    bytes=56 Sequence=1 hop limit=64  time = 1 ms
    Reply from 3003::1
    bytes=56 Sequence=2 hop limit=64  time = 1 ms
    Reply from 3003::1
    bytes=56 Sequence=3 hop limit=64  time = 1 ms
    Reply from 3003::1
    bytes=56 Sequence=4 hop limit=64  time = 1 ms
    Reply from 3003::1
    bytes=56 Sequence=5 hop limit=64  time = 1 ms

  --- 3003::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

Configuration files

- Switch A:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
```

```
interface Vlan-interface100
 ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 3002::1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::1/64
 tunnel-protocol ipv6-ipv4
 source Vlan-interface100
 destination 192.168.50.1
 service-loopback-group 1
#
 ipv6 route-static 3003:: 64 Tunnel0
#
```

- Switch B:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 192.168.50.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 3003::1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::2/64
 tunnel-protocol ipv6-ipv4
 source Vlan-interface100
 destination 192.168.100.1
 service-loopback-group 1
#
 ipv6 route-static 3002:: 64 Tunnel0
#
```

Example: Configuring a 6to4 tunnel

Applicable product matrix

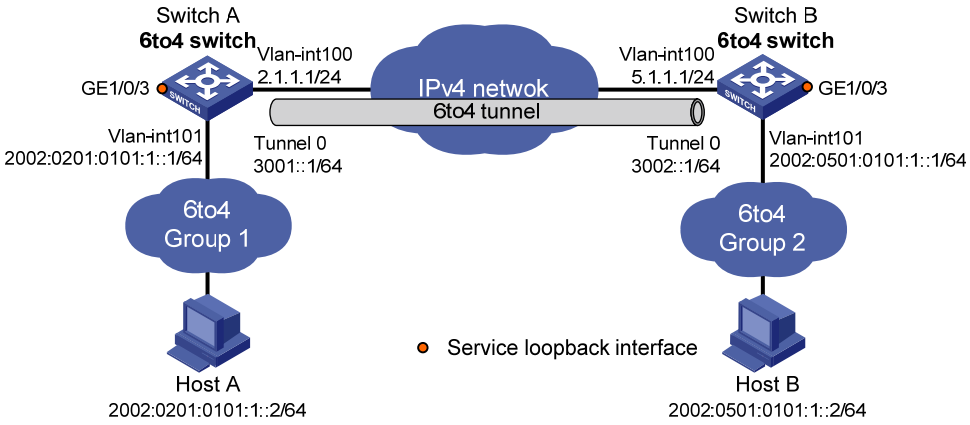
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 228, Switch A and Switch B can reach each other.

Configure a 6to4 tunnel between the 6to4 switches Switch A and Switch B so Host A and Host B can reach each other over the IPv4 network.

Figure 228 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ip address 2.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 2002:0201:0101:1::1/64
[SwitchA-Vlan-interface101] quit
```

Configure a 6to4 tunnel.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Configure a static route to 2002::/16 through the tunnel interface.

```
[SwitchA] ipv6 route-static 2002:: 16 tunnel 0
```

Configuring Switch B

Enable IPv6.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 5.1.1.1 24
[SwitchB-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2002:0501:0101:1::1/64
[SwitchB-Vlan-interface101] quit
```

Configure a 6to4 tunnel.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3002::1/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

Configure a static route to 2002::/16 through the tunnel interface.

```
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0
```

Verifying the configuration

Verify that the hosts can ping each other.

```
D:\>ping6 -s 2002:201:101:1::2 2002:501:101:1::2

Pinging 2002:501:101:1::2
from 2002:201:101:1::2 with 32 bytes of data:

Reply from 2002:501:101:1::2: bytes=32 time=13ms
Reply from 2002:501:101:1::2: bytes=32 time=1ms
Reply from 2002:501:101:1::2: bytes=32 time=1ms
Reply from 2002:501:101:1::2: bytes=32 time<1ms

Ping statistics for 2002:501:101:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

Configuration files

- Switch A:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 2
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 2.1.1.1 255.255.255.0
```

```
#
interface Vlan-interface101
 ipv6 address 2002:201:101:1::1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source Vlan-interface100
 service-loopback-group 1
#
 ipv6 route-static 2002:: 16 Tunnel0
#
```

- Switch B:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 2
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 5.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002:0501:0101:1::1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3002::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source Vlan-interface100
 service-loopback-group 1
#
 ipv6 route-static 2002:: 16 Tunnel0
#
```

Example: Configuring an ISATAP tunnel

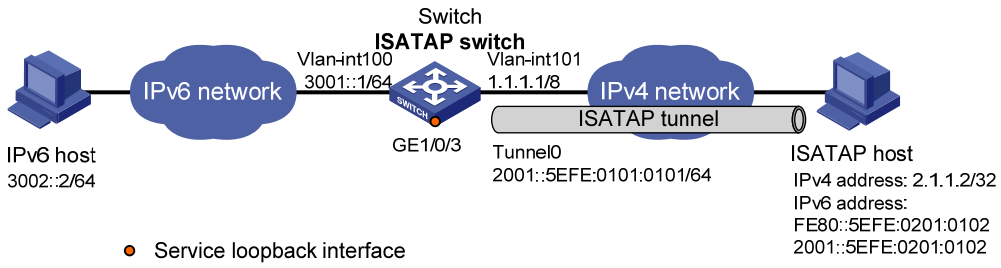
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 229, configure an ISATAP tunnel between the ISATAP switch and the ISATAP host so the ISATAP host in the IPv4 network can access the IPv6 network.

Figure 229 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring the ISATAP switch

Enable IPv6.

```
<Switch> system-view
[Switch] ipv6
```

Specify IP addresses for interfaces.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 3001::1/64
[Switch-Vlan-interface100] quit
[Switch] interface vlan-interface 101
[Switch-Vlan-interface101] ip address 1.1.1.1 255.0.0.0
[Switch-Vlan-interface101] quit
```

Configure an ISATAP tunnel.

```
[Switch] interface tunnel 0
[Switch-Tunnel0] ipv6 address 2001::/64 eui-64
[Switch-Tunnel0] source vlan-interface 101
[Switch-Tunnel0] tunnel-protocol ipv6-ipv4 isatap
```

Disable RA suppression so that the ISATAP host can obtain the address prefix carried in the RA message advertised by the ISATAP switch.

```
[Switch-Tunnel0] undo ipv6 nd ra halt
[Switch-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[Switch] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] undo stp enable
[Switch-GigabitEthernet1/0/3] undo lldp enable
[Switch-GigabitEthernet1/0/3] port service-loopback group 1
[Switch-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[Switch] interface tunnel 0
[Switch-Tunnel0] service-loopback-group 1
[Switch-Tunnel0] quit
```

Configuring the ISATAP host

Configurations on the ISATAP host vary with the operating systems. The following tasks are performed on Windows XP:

Install IPv6.

```
C:\>ipv6 install
```

On a host running Windows XP, the ISATAP interface is usually interface 2. Display information about the ISATAP interface.

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 0.0.0.0
  router link-layer address: 0.0.0.0
    preferred link-local fe80::5efe:2.1.1.2, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

Configure a route to the ISATAP switch.

```
C:\>netsh interface ipv6 isatap set router 1.1.1.1
```

Display information about the ISATAP interface.

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  uses Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 2.1.1.2
  router link-layer address: 1.1.1.1
    preferred global 2001::5efe:2.1.1.2, life 29d23h59m46s/6d23h59m46s (public)
    preferred link-local fe80::5efe:2.1.1.2, life infinite
  link MTU 1500 (true link MTU 65515)
  current hop limit 255
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

Verifying the configuration

Ping the IPv6 address of the tunnel interface on the switch to verify that an ISATAP tunnel has been established.

```
C:\>ping 2001::5efe:1.1.1.1

Pinging 2001::5efe:1.1.1.1 with 32 bytes of data:

Reply from 2001::5efe:1.1.1.1: time=1ms
Reply from 2001::5efe:1.1.1.1: time=1ms
Reply from 2001::5efe:1.1.1.1: time=1ms
Reply from 2001::5efe:1.1.1.1: time=1ms

Ping statistics for 2001::5efe:1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Verify that the IPv6 host can be pinged from the ISATAP host.

```
C:\>ping 3002::2

Pinging 3002::2 with 32 bytes of data:

Reply from 3002::2: time=4ms
Reply from 3002::2: time=1ms
Reply from 3002::2: time=1ms
Reply from 3002::2: time=1ms

Ping statistics for 3002::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

Configuration files

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 3001::1/64
#
interface Vlan-interface101
 ip address 1.1.1.1 255.0.0.0
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 2001::/64 eui-64
 undo ipv6 nd ra halt
 tunnel-protocol ipv6-ipv4 isatap
 source Vlan-interface101
 service-loopback-group 1
#
```

Example: Configuring an IPv4 over IPv4 tunnel

Applicable product matrix

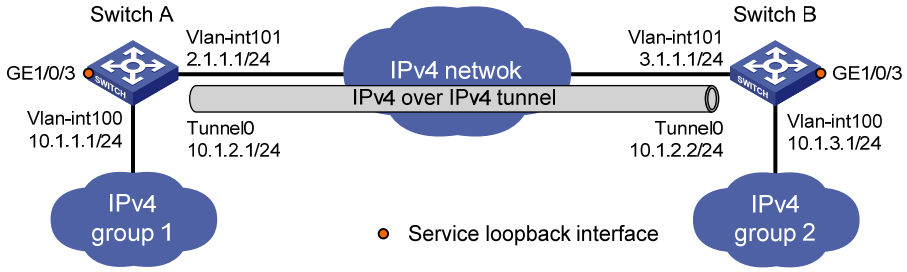
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 230, Switch A and Switch B can reach each other.

Configure an IPv4 over IPv4 tunnel between Switch A and Switch B so the two private IPv4 networks, group 1 and group 2, can reach each other over the IPv4 network.

Figure 230 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Specify an IPv4 address for VLAN-interface 100.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
```

Specify an IPv4 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ip address 2.1.1.1 255.255.255.0
[SwitchA-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchA] interface tunnel 0
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

Configure the tunnel encapsulation mode as IPv4 over IPv4.

```
[SwitchA-Tunnel0] tunnel-protocol ipv4-ipv4
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchA-Tunnel0] source 2.1.1.1
```

Specify the IP address of VLAN-interface 101 on Switch B as the destination address for the tunnel interface.

```
[SwitchA-Tunnel0] destination 3.1.1.1
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Configure a static route to IP network group 2 through the tunnel interface.

```
[SwitchA] ip route-static 10.1.3.0 255.255.255.0 tunnel 0
```

Configuring Switch B

Specify an IPv4 address for VLAN-interface 100.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.3.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
```

Specify an IPv4 address for VLAN-interface 101.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 3.1.1.1 255.255.255.0
[SwitchB-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchB] interface tunnel 0
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

Configure the tunnel encapsulation mode as IPv4 over IPv4.

```
[SwitchB-Tunnel0] tunnel-protocol ipv4-ipv4
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchB-Tunnel0] source 3.1.1.1
```

Specify the IP address of VLAN-interface 101 on Switch A as the destination address for the tunnel interface.

```
[SwitchB-Tunnel0] destination 2.1.1.1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
```

```
[SwitchB-Tunnel0] quit
```

Configure a static route to IP network group 1 through the tunnel interface.

```
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

Verifying the configuration

Display the status of the tunnel interface on Switch A.

```
<SwitchA> display interface tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1480
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1
Tunnel source 2.1.1.1, destination 3.1.1.1
Tunnel protocol/transport IP/IP
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  2 bytes/sec, 0 packets/sec
    4 packets input,  256 bytes
    0 input error
    12 packets output,  768 bytes
    0 output error
```

Display the status of the tunnel interface on Switch B.

```
<SwitchB> display interface tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1480
Internet Address is 10.1.2.2/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1
Tunnel source 3.1.1.1, destination 2.1.1.1
Tunnel protocol/transport IP/IP
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    5 packets input,  320 bytes
    0 input error
    9 packets output,  576 bytes
    0 output error
```

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch A.

```
[SwitchA] ping 10.1.3.1
  PING 10.1.3.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.3.1: bytes=56 Sequence=0 ttl=255 time=15 ms
    Reply from 10.1.3.1: bytes=56 Sequence=1 ttl=255 time=15 ms
    Reply from 10.1.3.1: bytes=56 Sequence=2 ttl=255 time=16 ms
```

```
  Reply from 10.1.3.1: bytes=56 Sequence=3 ttl=255 time=16 ms
  Reply from 10.1.3.1: bytes=56 Sequence=4 ttl=255 time=15 ms

--- 10.1.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/15/16 ms
```

Configuration files

- Switch A:

```
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ip address 2.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ip address 10.1.2.1 255.255.255.0
 tunnel-protocol ipv4-ipv4
 source 2.1.1.1
 destination 3.1.1.1
 service-loopback-group 1
#
 ip route-static 10.1.3.0 255.255.255.0 Tunnel0
#
```

- Switch B:

```
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface101
 ip address 3.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ip address 10.1.2.2 255.255.255.0
 tunnel-protocol ipv4-ipv4
 source 3.1.1.1
 destination 2.1.1.1
 service-loopback-group 1
#
 ip route-static 10.1.1.0 255.255.255.0 Tunnel0
#
```

Example: Configuring an IPv4 over IPv6 tunnel

Applicable product matrix

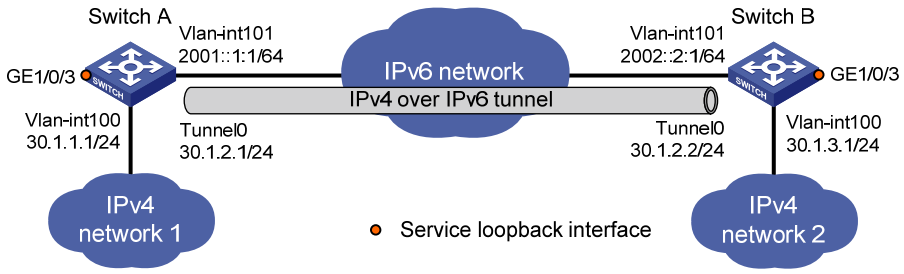
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 231, Switch A and Switch B can reach each other.

Configure an IPv4 over IPv6 tunnel between Switch A and Switch B so the two IPv4 networks can reach each other over the IPv6 network.

Figure 231 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 30.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 2001::1:1 64
[SwitchA-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchA] interface tunnel 0
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel0] ip address 30.1.2.1 255.255.255.0
```

Configure the tunnel encapsulation mode as IPv4 over IPv6.

```
[SwitchA-Tunnel0] tunnel-protocol ipv4-ipv6
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchA-Tunnel0] source 2001::1:1
```

Specify the IP address of VLAN-interface 101 on Switch B as the destination address for the tunnel interface.

```
[SwitchA-Tunnel0] destination 2002::2:1
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Configure a static route to network 2 through the tunnel interface.

```
[SwitchA] ip route-static 30.1.3.0 255.255.255.0 tunnel 0
```

Configuring Switch B

Enable IPv6.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 30.1.3.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2002::2:1 64
[SwitchB-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchB] interface tunnel 0
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel0] ip address 30.1.2.2 255.255.255.0
```

Configure the tunnel encapsulation mode as IPv4 over IPv6.

```
[SwitchB-Tunnel0] tunnel-protocol ipv4-ipv6
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchB-Tunnel0] source 2002::2:1
```

Specify the IP address of VLAN-interface 101 on Switch A as the destination address for the tunnel interface.

```
[SwitchB-Tunnel0] destination 2001::1:1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

Configure a static route to network 1 through the tunnel interface.

```
[SwitchB] ip route-static 30.1.1.0 255.255.255.0 tunnel 0
```

Verifying the configuration

Display the status of the tunnel interface on Switch A.

```
<SwitchA> display interface tunnel 0
Tunnel0 current state: UP
```

```
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1460
Internet Address is 30.1.2.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1
Tunnel source 2001::1:1, destination 2002::2:1
Tunnel protocol/transport IP/IPv6
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    152 packets input,  9728 bytes
    0 input error
    168 packets output,  10752 bytes
    0 output error
```

Display the status of the tunnel interface on Switch B.

```
<SwitchB> display interface tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1460
Internet Address is 30.1.2.2/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1
Tunnel source 2002::2:1, destination 2001::1:1
Tunnel protocol/transport IP/IPv6
Last clearing of counters:  Never
    Last 300 seconds input:  1 bytes/sec, 0 packets/sec
    Last 300 seconds output:  1 bytes/sec, 0 packets/sec
    167 packets input,  10688 bytes
    0 input error
    170 packets output,  10880 bytes
    0 output error
```

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch A.

```
[SwitchA] ping 30.1.3.1
  PING 30.1.3.1: 56  data bytes, press CTRL_C to break
    Reply from 30.1.3.1: bytes=56 Sequence=0 ttl=255 time=46 ms
    Reply from 30.1.3.1: bytes=56 Sequence=1 ttl=255 time=15 ms
    Reply from 30.1.3.1: bytes=56 Sequence=2 ttl=255 time=16 ms
    Reply from 30.1.3.1: bytes=56 Sequence=3 ttl=255 time=15 ms
    Reply from 30.1.3.1: bytes=56 Sequence=4 ttl=255 time=16 ms

  --- 30.1.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 15/21/46 ms
```

Configuration files

- Switch A:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 30.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2001::1:1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ip address 30.1.2.1 255.255.255.0
 tunnel-protocol ipv4-ipv6
 source 2001::1:1
 destination 2002::2:1
 service-loopback-group 1
#
ip route-static 30.1.3.0 255.255.255.0 Tunnel0
#
```

- Switch B:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 30.1.3.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002::2:1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
```

```
#
interface Tunnel0
 ip address 30.1.2.2 255.255.255.0
 tunnel-protocol ipv4-ipv6
 source 2002::2:1
 destination 2001::1:1
 service-loopback-group 1
#
ip route-static 30.1.1.0 255.255.255.0 Tunnel0
#
```

Example: Configuring an IPv6 over IPv6 tunnel

Applicable product matrix

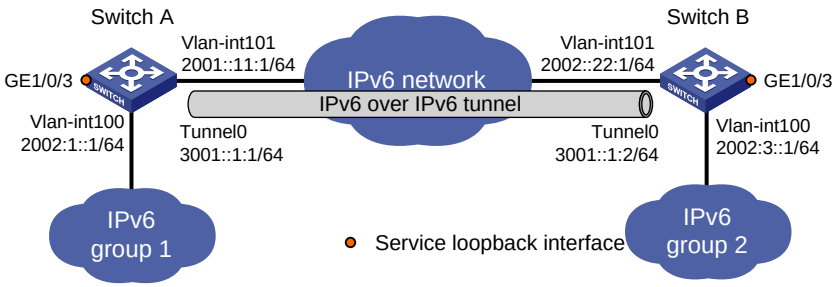
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 232, Switch A and Switch B can reach each other.

Configure an IPv6 over IPv6 tunnel between Switch A and Switch B so the two IPv6 networks can reach each other without disclosing their IPv6 addresses.

Figure 232 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

Specify an IPv6 address for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 address 2002:1::1 64
[SwitchA-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 2001::11:1 64
[SwitchA-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchA] interface tunnel 0
```

Specify an IPv6 address for the tunnel interface.

```
[SwitchA-Tunnel0] ipv6 address 3001::1:1 64
```

Configure the tunnel encapsulation mode as IPv6 over IPv6.

```
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv6
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchA-Tunnel0] source 2001::11:1
```

Specify the IP address of VLAN-interface 101 on Switch B as the destination address for the tunnel interface.

```
[SwitchA-Tunnel0] destination 2002::22:1
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Configure a static route to IPv6 network group 2 through the tunnel interface.

```
[SwitchA] ipv6 route-static 2002:3:: 64 tunnel 0
```

Configuring Switch B

Enable IPv6.

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

Specify an IPv6 address for VLAN-interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ipv6 address 2002:3::1 64
[SwitchB-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2002::22:1 64
[SwitchB-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchB] interface tunnel 0
```

Specify an IPv6 address for the tunnel interface.

```
[SwitchB-Tunnel0] ipv6 address 3001::1:2 64
```

Configure the tunnel encapsulation mode as IPv6 over IPv6.

```
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv6
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchB-Tunnel0] source 2002::22:1
```

Specify the IP address of VLAN-interface 101 on Switch A as the destination address for the tunnel interface.

```
[SwitchB-Tunnel0] destination 2001::11:1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

Configure a static route to IPv6 network group 1 through the tunnel interface.

```
[SwitchB] ipv6 route-static 2002:1:: 64 tunnel 0
```

Verifying the configuration

Display the status of the tunnel interface on Switch A.

```
<SwitchA> display ipv6 interface tunnel 0 verbose
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::2013:1
  Global unicast address(es):
```

```
    3001::1:1, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF13:1
    FF02::1:FF01:1
    FF02::1:FF00:0
    FF02::2
    FF02::1
  MTU is 1460 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
…
```

Display the status of the tunnel interface on Switch B.

```
<SwitchB> display ipv6 interface tunnel 0 verbose
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::2024:1
  Global unicast address(es):
    3001::1:2, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF24:1
    FF02::1:FF01:2
    FF02::1:FF00:0
    FF02::2
    FF02::1
  MTU is 1460 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
…
```

Ping the IPv6 address of the peer interface VLAN-interface 100 from Switch A.

```
[SwitchA] ping ipv6 2002:3::1
  PING 2002:3::1 : 56  data bytes, press CTRL_C to break
    Reply from 2002:3::1
    bytes=56 Sequence=1 hop limit=64  time = 31 ms
    Reply from 2002:3::1
    bytes=56 Sequence=2 hop limit=64  time = 1 ms
    Reply from 2002:3::1
    bytes=56 Sequence=3 hop limit=64  time = 16 ms
    Reply from 2002:3::1
    bytes=56 Sequence=4 hop limit=64  time = 16 ms
    Reply from 2002:3::1
    bytes=56 Sequence=5 hop limit=64  time = 31 ms

  --- 2002:3::1 ping statistics ---
    5 packet(s) transmitted
```

```
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/19/31 ms
```

Configuration files

- SwitchA:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 2002:1::1/64
#
interface Vlan-interface101
 ipv6 address 2001::11:1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::1:1/64
 tunnel-protocol ipv6-ipv6
 source 2001::11:1
 destination 2002::22:1
 service-loopback-group 1
#
ipv6 route-static 2002:3:: 64 Tunnel0
#
```

- SwitchB:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 2002:3::1/64
#
interface Vlan-interface101
 ipv6 address 2002::22:1/64
#
```

```
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::1:2/64
 tunnel-protocol ipv6-ipv6
 source 2002::2:1
 destination 2001::11:1
 service-loopback-group 1
#
ipv6 route-static 2002:1:: 64 Tunnel0
#
```

Example: Configuring a GRE over IPv4 tunnel

Applicable product matrix

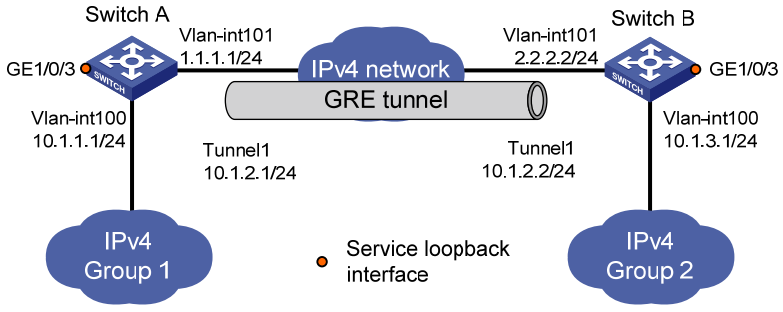
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 233, Switch A and Switch B can reach each other.

Configure a GRE over IPv4 tunnel between Switch A and Switch B so the two private IPv4 networks, Group 1 and Group 2, can reach each other over the IPv4 network.

Figure 233 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Specify IP addresses for interfaces.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ip address 1.1.1.1 255.255.255.0
[SwitchA-Vlan-interface101] quit
```

Create tunnel interface Tunnel 1.

```
[SwitchA] interface tunnel 1
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel1] ip address 10.1.2.1 255.255.255.0
```

Configure the tunnel encapsulation mode as GRE over IPv4.

```
[SwitchA-Tunnel1] tunnel-protocol gre
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchA-Tunnel1] source vlan-interface 101
```

Specify the IP address of VLAN-interface 101 on Switch B as the destination address for the tunnel interface.

```
[SwitchA-Tunnel1] destination 2.2.2.2
[SwitchA-Tunnel1] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 1
[SwitchA-Tunnel1] service-loopback-group 1
[SwitchA-Tunnel1] quit
```

Configure a static route to IP network Group 2 through the tunnel interface.

```
[SwitchA] ip route-static 10.1.3.0 255.255.255.0 tunnel 1
```

Configuring Switch B

Specify IP addresses for interfaces.

```
<SwitchB> system-view
```

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.3.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 2.2.2.2 255.255.255.0
[SwitchB-Vlan-interface101] quit
```

Create tunnel interface Tunnel 1.

```
[SwitchB] interface tunnel 1
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel1] ip address 10.1.2.2 255.255.255.0
```

Configure the tunnel encapsulation mode as GRE over IPv4.

```
[SwitchB-Tunnel1] tunnel-protocol gre
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchB-Tunnel1] source vlan-interface 101
```

Specify the IP address of VLAN-interface 101 on Switch A as the destination address for the tunnel interface.

```
[SwitchB-Tunnel1] destination 1.1.1.1
[SwitchB-Tunnel1] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 1
[SwitchB-Tunnel1] service-loopback-group 1
[SwitchB-Tunnel1] quit
```

Configure a static route to IP network Group 1 through the tunnel interface.

```
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 Tunnel 1
```

Verifying the configuration

Display the status of the tunnel interface on Switch A.

```
[SwitchA] display interface tunnel 1
Tunnel1 current state: UP
Line protocol current state: UP
Description: Tunnel1 Interface
The Maximum Transmit Unit is 1476
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1.
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel bandwidth 64 (kbps)
```

```
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    10 packets input,  840 bytes
    0 input error
    10 packets output,  840 bytes
    0 output error
```

Display the status of the tunnel interface on Switch B.

```
[SwitchB] display interface tunnel 1
Tunnel1 current state: UP
Line protocol current state: UP
Description: Tunnel1 Interface
The Maximum Transmit Unit is 1476
Internet Address is 10.1.2.2/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1.
Tunnel source 2.2.2.2, destination 1.1.1.1
Tunnel bandwidth 64 (kbps)
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters:  Never
    Last 300 seconds input:  2 bytes/sec, 0 packets/sec
    Last 300 seconds output:  2 bytes/sec, 0 packets/sec
    10 packets input,  840 bytes
    0 input error
    10 packets output,  840 bytes
    0 output error
```

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch B.

```
[SwitchB] ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=0 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=2 ms

  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
```

Configuration files

- SwitchA:

```
 #
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel1
 ip address 10.1.2.1 255.255.255.0
 source Vlan-interface101
 destination 2.2.2.2
 service-loopback-group 1
#
 ip route-static 10.1.3.0 255.255.255.0 Tunnel1
#
```

- Switch B:

```
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface101
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel1
 ip address 10.1.2.2 255.255.255.0
 source Vlan-interface101
 destination 1.1.1.1
```

```
 service-loopback-group 1
#
 ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
```

Example: Configuring a GRE over IPv6 tunnel

Applicable product matrix

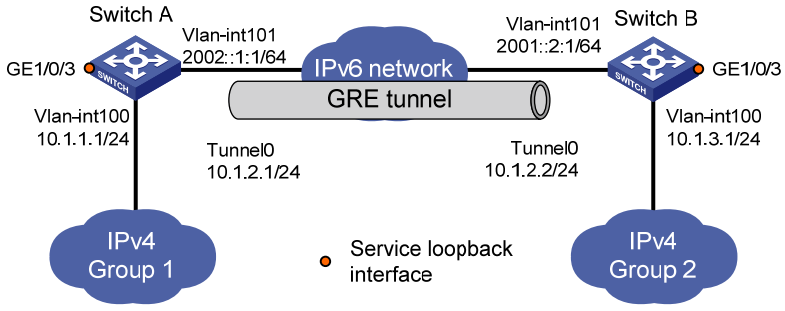
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 234, Switch A and Switch B can reach each other.

Configure a GRE over IPv6 tunnel between Switch A and Switch B so the two private IPv4 networks, Group1 and Group 2, can reach other over the IPv6 network.

Figure 234 Network diagram



Configuration restrictions and guidelines

Before you configure a tunnel interface, do the following:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

Configuration procedures

Configuring Switch A

Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchA] vlan 100
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] vlan 101
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 2002::1:1 64
[SwitchA-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchA] interface tunnel 0
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

Configure the tunnel encapsulation mode as GRE over IPv6.

```
[SwitchA-Tunnel0] tunnel-protocol gre ipv6
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchA-Tunnel0] source 2002::1:1
```

Specify the IP address of VLAN-interface 101 on Switch B as the destination address for the tunnel interface.

```
[SwitchA-Tunnel0] destination 2001::2:1
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

Configure a static route to IP network Group 2 through the tunnel interface.

```
[SwitchA] ip route-static 10.1.3.0 255.255.255.0 tunnel 0
```

Configuring Switch B

Enable IPv6.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Specify an IPv4 address for VLAN-interface 100.

```
[SwitchB] vlan 100
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.3.1 255.255.255.0
```

```
[SwitchB-Vlan-interface100] quit
```

Specify an IPv6 address for VLAN-interface 101.

```
[SwitchB] vlan 101
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2001::2:1 64
[SwitchB-Vlan-interface101] quit
```

Create tunnel interface Tunnel 0.

```
[SwitchB] interface tunnel 0
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

Configure the tunnel encapsulation mode as GRE over IPv6.

```
[SwitchB-Tunnel0] tunnel-protocol gre ipv6
```

Specify the IP address of VLAN-interface 101 as the source address for the tunnel interface.

```
[SwitchB-Tunnel0] source 2001::2:1
```

Specify the IP address of VLAN-interface 101 on Switch A as the destination address for the tunnel interface.

```
[SwitchB-Tunnel0] destination 2002::1:1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to service loopback group 1. Disable STP and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

Configure a static route to IP network Group 1 through the tunnel interface.

```
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

Verifying the configuration

Display the status of the tunnel interface on Switch A.

```
[SwitchA] display interface Tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1456
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1.
Tunnel source 2002::1:1, destination 2001::2:1
```

```
Tunnel protocol/transport GRE/IPv6
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    10 packets input,  840 bytes
    0 input error
    10 packets output,  840 bytes
    0 output error
```

Display the status of the tunnel interface on Switch B.

```
[SwitchB] display interface Tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1456
Internet Address is 10.1.2.2/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1.
Tunnel source 2001::2:1, destination 2002::1:1
Tunnel protocol/transport GRE/IPv6
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    10 packets input,  840 bytes
    0 input error
    10 packets output,  840 bytes
    0 output error
```

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch B.

```
[SwitchB] ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=0 ttl=255 time=3 ms
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms

  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms
```

Configuration files

- Switch A:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002::1:1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ip address 10.1.2.1 255.255.255.0
 tunnel-protocol gre ipv6
 source 2002::1:1
 destination 2002::2:1
 service-loopback-group 1
#
ip route-static 10.1.3.0 255.255.255.0 Tunnel0
#
```

- Switch B:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002::2:1/64
#
interface GigabitEthernet1/0/3
 stp disable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ip address 10.1.2.2 255.255.255.0
```

```
 tunnel-protocol gre ipv6
 source 2002::2:1
 destination 2002::1:1
 service-loopback-group 1
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel0
#
```

UDP helper configuration examples

This chapter provides a UDP helper configuration example.

Example: Configuring UDP helper

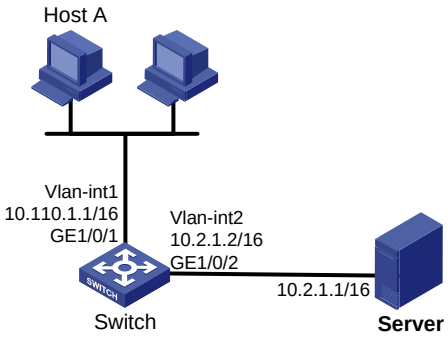
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 235, configure UDP helper on the switch to forward broadcast packets with UDP destination port number 55 and destination IP address 255.255.255.255 from Host A to the destination server 10.2.1.1/16.

Figure 235 Network diagram



Configuration restrictions and guidelines

The device cannot receive directed broadcasts by default. To use UDP helper on the device, use the **ip forward-broadcast** command in system view.

Configuration procedures

Create VLAN-interface 1, and assign IP address 10.110.1.1/16 to the interface.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-vlan-interface1] ip address 10.110.1.1 16
```

```
[Switch-vlan-interface1] quit
```

Create VLAN 2.

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

Assign GigabitEthernet 1/0/2 to VLAN 2.

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port access vlan 2
[Switch-GigabitEthernet1/0/2] quit
```

Create VLAN-interface 2, and assign IP address 10.2.1.2/16 to the interface.

```
[Switch] interface vlan-interface 2
[Switch-vlan-interface2] ip address 10.2.1.2 16
[Switch-vlan-interface2] quit
```

Enable the switch to receive directed broadcasts.

```
[Switch] ip forward-broadcast
```

Enable UDP helper.

```
[Switch] udp-helper enable
```

Enable UDP helper to forward broadcast packets with the UDP destination port 55.

```
[Switch] udp-helper port 55
```

Specify the destination server 10.2.1.1 on VLAN-interface 1.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] udp-helper server 10.2.1.1
```

Verifying the configuration

Display information about packets forwarded by UDP helper on VLAN-interface 1 destined for server 10.2.1.1.

```
[Switch] display udp-helper server
Interface name          Server VPN                  Server address  Packets
Vlan1                                               10.2.1.1        0
```

Configuration files

```
#
 udp-helper enable
 udp-helper port 55
#
 ip forward-broadcast
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 10.110.1.1 255.255.0.0
 udp-helper server 10.2.1.1
```

```
#
interface Vlan-interface2
 ip address 10.2.1.2 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

URPF configuration examples

This chapter provides Unicast Reverse Path Forwarding (URPF) configuration examples.

URPF protects a network against source spoofing attacks. It supports the following check modes:

- **Strict URPF**—To pass strict URPF check, the source address of a packet and the receiving interface must match the destination address and output interface of a FIB entry. Strict URPF is often deployed between a PE device and a CE device.
- **Loose URPF**—To pass loose URPF check, the source address of a packet must match the destination address of a FIB entry. Loose URPF is often deployed between ISPs, especially in the case of asymmetrical routing.

Example: Configuring URPF

Applicable product matrix

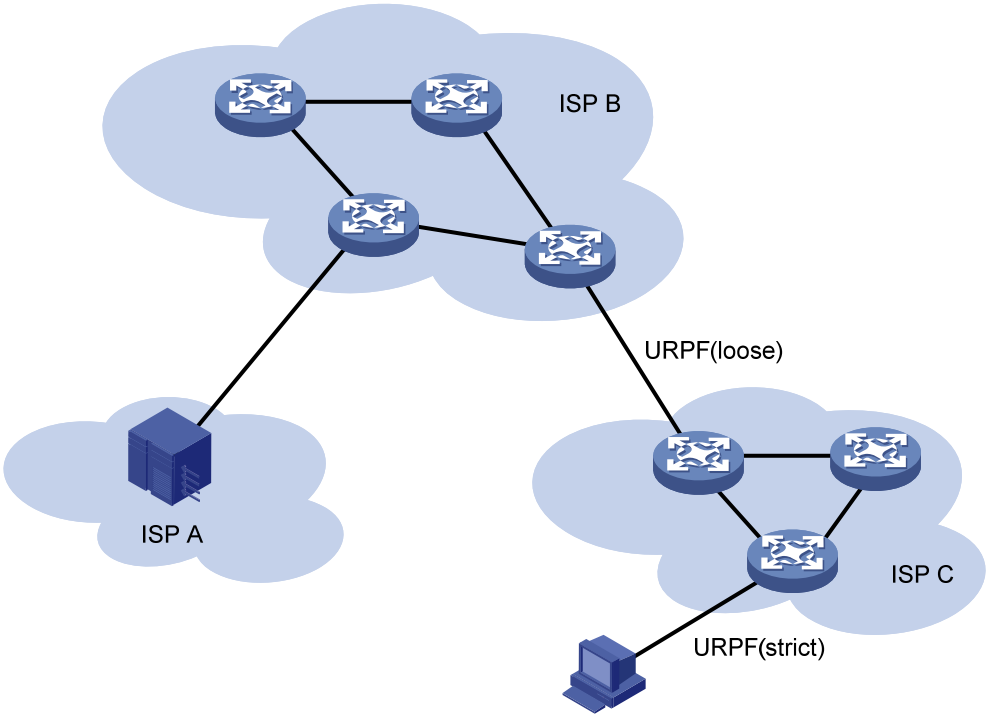
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 236:

- Enable URPF on the egress device of ISP B network to allow packets with source address matching the destination address of a FIB entry from ISP C network to pass.
- Enable URPF on the egress device of ISP C network to allow packets with source address and receiving interface matching the destination address and output interface of a FIB entry from the client to pass.

Figure 236 Network diagram



Configuration restrictions and guidelines

When the number of routes on the switch exceeds half of the routing table capacity, the URPF function cannot be enabled.

Configuration procedures

Configure strict URPF check.

```
<Switch> system-view
[Switch] ip urpf strict
```

Configure loose URPF check.

```
<Switch> system-view
[Switch] ip urpf loose
```

Verifying the configuration

If strict URPF check is enabled, a packet passes the check when its source address and receiving interface match the destination address and output interface of a FIB entry. You can use the **display fib** command to display FIB entries.

If loose URPF check enabled, a packet passes the check if its source address matches the destination address of a FIB entry. You can use the **display fib** command to display the FIB entry.

Configuration files

```
#
 ip urpf strict
#
 ip urpf loose
#
```

VLAN configuration examples

This chapter provides VLAN configuration examples.

Example: Configuring port-based VLANs and VLAN-interfaces

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6670

Network requirements

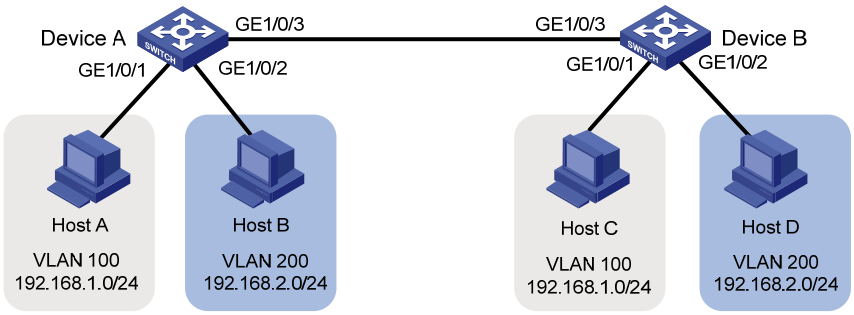
As shown in Figure 237:

- To confine broadcast traffic and ensure community security, a company uses the VLAN feature to isolate Layer 2 traffic from different departments. The company assigns VLAN 100 to department A and VLAN 200 to department B.
- The users in department A are on the IP network segment 192.168.1.0/24, and they are configured with the gateway IP address 192.168.1.1. The users in department B are on the network segment 192.168.2.0/24, and they are configured with the gateway IP address 192.168.2.1.

Configure port-based VLANs and VLAN-interfaces, so that:

- The hosts in the same VLAN can communicate at Layer 2. The hosts in different VLANs cannot communicate at Layer 2, but they can communicate at Layer 3.
- Configure Device A as the gateway for users in department A, and configure Device B as the gateway for users in department B.

Figure 237 Network diagram



Configuration procedures

Configuring Device A

Create VLAN 100, and assign port GigabitEthernet 1/0/1 to VLAN 100.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

Create VLAN-interface 100, and configure its IP address as 192.168.1.1/24.

```
[DeviceA] interface Vlan-interface 100
[DeviceA-Vlan-interface100] ip address 192.168.1.1 24
[DeviceA-Vlan-interface100] quit
```

Create VLAN 200, and assign port GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

Create VLAN-interface 200, and configure its IP address as 192.168.2.2/24.

```
[DeviceA] interface Vlan-interface 200
[DeviceA-Vlan-interface200] ip address 192.168.2.2 24
[DeviceA-Vlan-interface200] quit
```

Configure port GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLAN 100 and VLAN 200.

```
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

Remove the port from VLAN 1, so that the port can forward packets from VLAN 100 and VLAN 200.

```
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring Device B

Create VLAN 100, and assign port GigabitEthernet 1/0/1 to VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/1
[DeviceB-vlan100] quit
```

Create VLAN-interface 100, and configure its IP address as 192.168.1.2/24.

```
[DeviceB] interface Vlan-interface 100
[DeviceB-Vlan-interface100] ip address 192.168.1.2 24
[DeviceB-Vlan-interface100] quit
```

Create VLAN 200, and assign port GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/2
[DeviceB-vlan200] quit
```

Create VLAN-interface 200, and configure its IP address as 192.168.2.1/24.

```
[DeviceB] interface Vlan-interface 200
[DeviceB-Vlan-interface200] ip address 192.168.2.1 24
[DeviceB-Vlan-interface200] quit
```

Configure port GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLAN 100 and VLAN 200.

```
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

Remove the port from VLAN 1, so that the port can forward packets from VLAN 100 and VLAN 200.

```
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] quit
```

Verifying the configuration

1. Use the **display vlan** command to display the VLAN information and verify whether the configuration succeeds. This section uses VLAN 100 and VLAN 200 on Device A as an example.

```
[DeviceA] display vlan 100
 VLAN ID: 100
 VLAN Type: static
 Route Interface: configured
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged   Ports:
    GigabitEthernet1/0/3
 Untagged Ports:
    GigabitEthernet1/0/1
[DeviceA] display vlan 200
 VLAN ID: 200
 VLAN Type: static
 Route Interface: configured
 IP Address: 192.168.2.2
 Subnet Mask: 255.255.255.0
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged   Ports:
    GigabitEthernet1/0/3
 Untagged Ports:
GigabitEthernet1/0/2
```

2. Perform ping operations between Host A and Host B. View the ARP tables of Host A and Host B.

   Host A and Host B can ping each other. In the ARP table of Host A, an entry containing the IP address and MAC address of Host C exists. In the ARP table of Host B, an entry containing the IP address and MAC address of Host A exists.

3. Perform ping operations between Host A and Host D. View the ARP tables of Host A and Host D.

Host A and Host D can ping each other. In the ARP table of Host A, no ARP entry for Host D exists. In the ARP table of Host D, no ARP entry for Host A exists.

Configuration files

- Device A:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

- Device B:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

Example: Configuring a super VLAN

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620
	Release series 6630
	Release series 6670

Network requirements

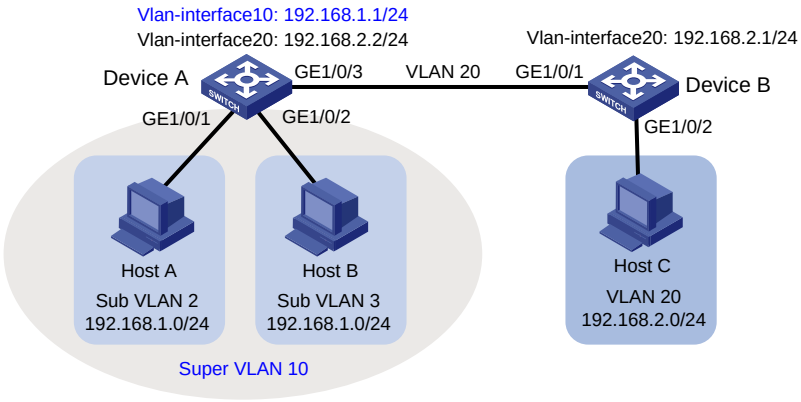
As shown in Figure 238:

- Users in VLAN 2 access the network through GigabitEthernet 1/0/1 of Device A, and users in VLAN 3 access the network through GigabitEthernet 1/0/2 of Device A.
- GigabitEthernet 1/0/3 of Device A and GigabitEthernet 1/0/1 of Device B belong to VLAN 20.
- The terminal users in VLAN 20 use IP addresses on the IP network segment 192.168.2.0/24, and they use 192.168.2.1 as the gateway IP address.

Configure a super VLAN so that:

- The terminal users in VLAN 2 and VLAN 3 use IP addresses on the IP network segment 192.168.1.0/24, and they use 192.168.1.1 as the gateway IP address.
- Terminal users in VLAN 2, VLAN 3, and VLAN 20 are isolated at Layer 2, and they can communicate with each other at Layer 3.

Figure 238 Network diagram



Configuration restrictions and guidelines

You cannot assign physical ports to a super VLAN. A VLAN that contains physical ports cannot be configured as a super VLAN.

Configuration procedures

Configuring Device A

Create VLAN 10, and configure the VLAN as a super VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] quit
```

Create VLAN 2, and assign port GigabitEthernet 1/0/1 to VLAN 2.

```
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

Create VLAN 3, and assign port GigabitEthernet 1/0/2 to VLAN 3.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
```

Associate the super VLAN 10 with sub VLANs 2 and 3.

```
[DeviceA] vlan 10
[DeviceA-vlan10] subvlan 2 3
[DeviceA-vlan10] quit
```

Create a VLAN interface for super VLAN 10.

```
[DeviceA] interface vlan-interface 10
```

Configure an IP address for the VLAN interface.

```
[DeviceA-Vlan-interface10] ip address 192.168.1.1 24
```

Enable local proxy ARP for the VLAN interface.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
```

```
[DeviceA-Vlan-interface10] quit
```

Create VLAN 20.

```
[DeviceA] vlan 20
[DeviceA-vlan20] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
```

Remove it from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign it to VLAN 20.

```
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 20
```

Create a VLAN-interface for VLAN 20, and configure an IP address for the VLAN-interface.

```
[DeviceA] interface Vlan-interface 20
[DeviceA-Vlan-interface20] ip address 192.168.2.2 24
[DeviceA-Vlan-interface20] quit
```

Configuring Device B

Create VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Remove it from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Assign it to VLAN 20.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20
```

Assign GigabitEthernet 1/0/2 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/2
[DeviceB-vlan20] quit
```

Create a VLAN-interface for VLAN 20, and configure an IP address for the VLAN-interface.

```
[DeviceB] interface Vlan-interface 20
[DeviceB-Vlan-interface20] ip address 192.168.2.1 24
[DeviceB-Vlan-interface20] quit
```

Verifying the configuration

1. Display the super VLAN configuration information.

```
[DeviceA] display supervlan
 SuperVLAN ID :  10
 SubVLAN ID :  2 3

 VLAN ID: 10
 VLAN Type: static
```

```
 It is a Super VLAN.
 Route Interface: configured
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged   Ports: none
 Untagged Ports: none

 VLAN ID: 2
 VLAN Type: static
 It is a Sub VLAN.
 Route Interface: configured
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1

 VLAN ID: 3
 VLAN Type: static
 It is a Sub VLAN.
 Route Interface: configured
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged   Ports: none
 Untagged Ports:
GigabitEthernet1/0/2
```

2. Perform ping operations between Host A and Host B. View the ARP tables of Host A and Host B.

   Host A and Host B can ping each other. In the ARP table of Host A, the IP address of Host B corresponds to the MAC address of VLAN-interface 10. In the ARP table of Host B, the IP address of Host A corresponds to the MAC address of VLAN-interface 10.

3. Perform ping operations between Host A and Host C. View the ARP tables of Host A and Host C.

   Host A and Host C can ping each other. In the ARP table of Host A, no entry about Host C exists. In the ARP table of Host C, no entry about Host A exists.

Configuration files

- Device A:

```
#
vlan 2
#
vlan 3
```

```
#
vlan 10
 supervlan
 subvlan 2 3
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
 local-proxy-arp enable
#
interface Vlan-interface20
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
```

- Device B:

```
#
vlan 20
#
interface Vlan-interface20
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

VLAN mapping configuration examples

This chapter provides VLAN mapping configuration examples.

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

- **One-to-one VLAN mapping**—Replaces one VLAN tag with another.
- **Two-to-two VLAN mapping**—Replaces the outer and inner VLAN tags of double tagged traffic with a new pair of VLAN tags.

Example: Configuring one-to-one VLAN mapping

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 239:

- Two branches of a company, Site 1 and Site 2, communicate with each other through the service provider network. The company uses CVLAN 10 to transmit voice traffic and uses CVLAN 20 to transmit data traffic.
- PE 1 and PE 2 are the edge devices of the service provider network. The service provider allocates only SVLAN 100 and SVLAN 200 to the company for transmitting data.

Configure one-to-one VLAN mapping, so that Site 1 and Site 2 can use SVLAN 100 and SVLAN 200 to transmit the voice traffic and data traffic, respectively, between the two branches. Figure 240 shows the effect of the one-to-one VLAN mapping.

Figure 239 Network diagram

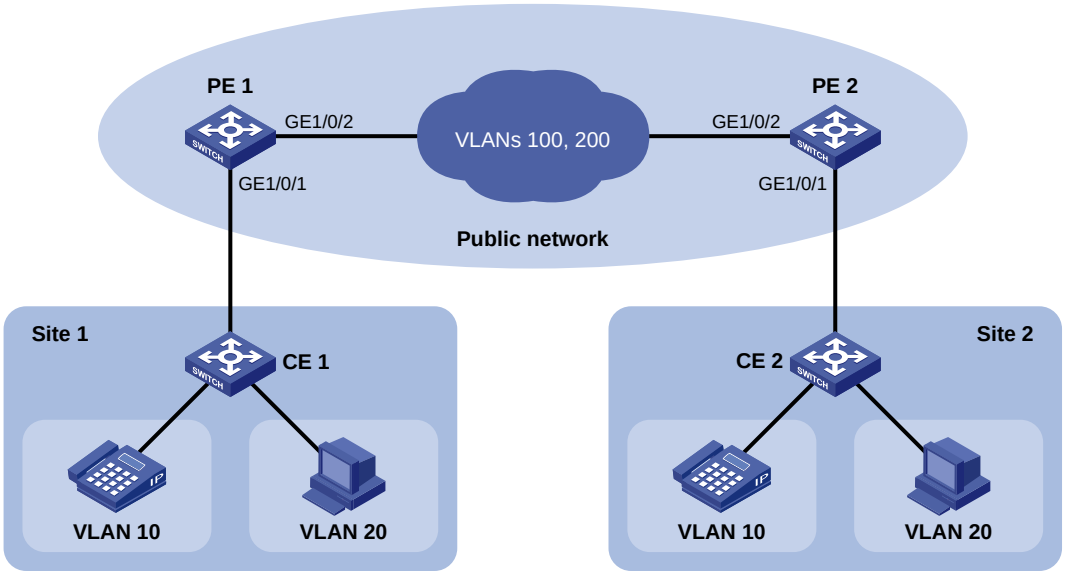
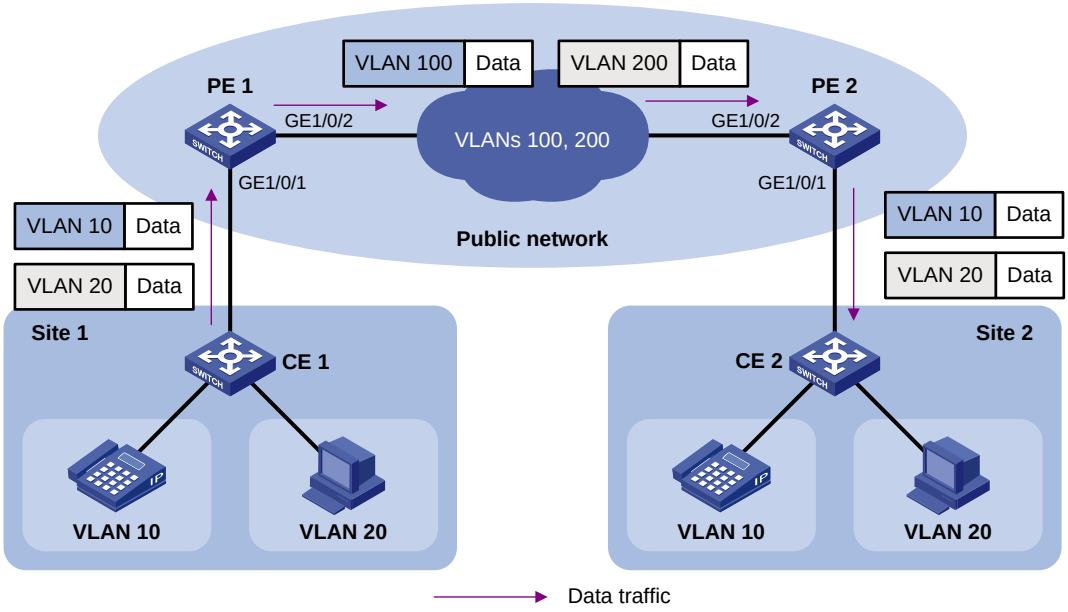


Figure 240 Effect of one-to-one VLAN mapping



Configuration restrictions and guidelines

When you configure one-to-one VLAN mapping, you must enable basic QinQ on the customer-side ports.

Configuration procedures

Configuring PE 1

1. Create the CVLANs and SVLANs used in this example.

```
<PE1> system-view
```

```
[PE1] vlan 10
[PE1-vlan10] quit
[PE1] vlan 20
[PE1-vlan20] quit
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] vlan 200
[PE1-vlan200] quit
```

2. Configure an uplink policy:

Configure a class named **uplink10** to match the traffic from CVLAN 10 of Site 1.

```
[PE1] traffic classifier uplink10
[PE1-classifier-uplink10] if-match customer-vlan-id 10
[PE1-classifier-uplink10] quit
```

Configure a behavior named **remark_to_100** to mark traffic with SVLAN tag 100.

```
[PE1] traffic behavior remark_to_100
[PE1-behavior-remark_to_100] remark service-vlan-id 100
[PE1-behavior-remark_to_100] quit
```

Configure a class named **uplink20** to match the traffic from CVLAN 20.

```
[PE1] traffic classifier uplink20
[PE1-classifier-uplink20] if-match customer-vlan-id 20
[PE1-classifier-uplink20] quit
```

Configure a behavior named **remark_to_200** to mark traffic with SVLAN tag 200.

```
[PE1] traffic behavior remark_to_200
[PE1-behavior-remark_to_200] remark service-vlan-id 200
[PE1-behavior-remark_to_200] quit
```

Create a QoS policy named **uplink**.

```
[PE1] qos policy uplink
```

Associate class **uplink10** with behavior **remark_to_100**.

```
[PE1-qospolicy-uplink] classifier uplink10 behavior remark_to_100
```

Associate class **uplink20** with behavior **remark_to_200**.

```
[PE1-qospolicy-uplink] classifier uplink20 behavior remark_to_200
[PE1-qospolicy-uplink] quit
```

3. Configure a downlink policy:

Configure a class named **downlink100** to match the traffic from SVLAN 100.

```
[PE1] traffic classifier downlink100
[PE1-classifier-downlink100] if-match service-vlan-id 100
[PE1-classifier-downlink100] quit
```

Configure a behavior named **remark_to_10** to mark traffic with CVLAN tag 10.

```
[PE1] traffic behavior remark_to_10
[PE1-behavior-remark_to_10] remark customer-vlan-id 10
[PE1-behavior-remark_to_10] quit
```

Configure a class named **downlink200** to match the traffic from CVLAN 200.

```
[PE1] traffic classifier downlink200
[PE1-classifier-downlink200] if-match service-vlan-id 200
[PE1-classifier-downlink200] quit
```

Configure a behavior named **remark_to_20** to mark traffic with CVLAN tag 20.

```
[PE1] traffic behavior remark_to_20
[PE1-behavior-remark_to_20] remark customer-vlan-id 20
[PE1-behavior-remark_to_20] quit
```

Create a QoS policy named **downlink**.

```
[PE1] qos policy downlink
```

Associate class **downlink100** with behavior **remark_to_10**.

```
[PE1-qospolicy-downlink] classifier downlink100 behavior remark_to_10
```

Associate class **downlink200** with behavior **remark_to_20**.

```
[PE1-qospolicy-downlink] classifier downlink200 behavior remark_to_20
[PE1-qospolicy-downlink] quit
```

4. Configure the customer-side port GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
```

Configure GigabitEthernet 1/0/1 to permit the packets from VLANs 10, 20, 100, and 200 to pass through tagged.

```
[PE1-GigabitEthernet1/0/1] port hybrid vlan 10 20 100 200 tagged
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[PE1-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Enable basic QinQ on GigabitEthernet 1/0/1.

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

Apply the policy named **uplink** to the incoming traffic of GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qos apply policy uplink inbound
```

Apply the policy named **downlink** to the outgoing traffic of GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qos apply policy downlink outbound
[PE1-GigabitEthernet1/0/1] quit
```

5. Configure the network-side port GigabitEthernet 1/0/2:

Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.

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

Assign GigabitEthernet 1/0/2 to VLANs 100 and 200.

```
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[PE1-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE1-GigabitEthernet1/0/2] quit
```

Configuring PE 2

1. Create the CVLANs and SVLANs used in this example.

```
<PE2> system-view
[PE2] vlan 10
[PE2-vlan10] quit
[PE2] vlan 20
[PE2-vlan20] quit
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] vlan 200
```

```
[PE2-vlan200] quit
```

2. Configure an uplink policy:

   # Configure a class named **uplink10** to match the traffic from CVLAN 10 of Site 2.

```
[PE2] traffic classifier uplink10
[PE2-classifier-uplink10] if-match customer-vlan-id 10
[PE2-classifier-uplink10] quit
```

   # Configure a behavior named **remark_to_100** to mark traffic with SVLAN tag 100.

```
[PE2] traffic behavior remark_to_100
[PE2-behavior-remark_to_100] remark service-vlan-id 100
[PE2-behavior-remark_to_100] quit
```

   # Configure a class named **uplink20** to match the traffic from CVLAN 20.

```
[PE2] traffic classifier uplink20
[PE2-classifier-uplink20] if-match customer-vlan-id 20
[PE2-classifier-uplink20] quit
```

   # Configure a behavior named **remark_to_200** to mark traffic with SVLAN tag 200.

```
[PE2] traffic behavior remark_to_200
[PE2-behavior-remark_to_200] remark service-vlan-id 200
[PE2-behavior-remark_to_200] quit
```

   # Create a QoS policy named **uplink**.

```
[PE2] qos policy uplink
```

   # Associate class **uplink10** with behavior **remark_to_100**.

```
[PE2-qospolicy-uplink] classifier uplink10 behavior remark_to_100
```

   # Associate class **uplink20** with behavior **remark_to_200**.

```
[PE2-qospolicy-uplink] classifier uplink20 behavior remark_to_200
[PE2-qospolicy-uplink] quit
```

3. Configure a downlink policy:

   # Configure a class named **downlink100** to match the traffic from SVLAN 100.

```
[PE2] traffic classifier downlink100
[PE2-classifier-downlink100] if-match service-vlan-id 100
[PE2-classifier-downlink100] quit
```

   # Configure a behavior named **remark_to_10** to mark traffic with CVLAN tag 10.

```
[PE2] traffic behavior remark_to_10
[PE2-behavior-remark_to_10] remark customer-vlan-id 10
[PE2-behavior-remark_to_10] quit
```

   # Configure a class named **downlink200** to match the traffic from CVLAN 200.

```
[PE2] traffic classifier downlink200
[PE2-classifier-downlink200] if-match service-vlan-id 200
[PE2-classifier-downlink200] quit
```

   # Configure a behavior named **remark_to_20** to mark traffic with CVLAN tag 20.

```
[PE2] traffic behavior remark_to_20
[PE2-behavior-remark_to_20] remark customer-vlan-id 20
[PE2-behavior-remark_to_20] quit
```

   # Create a QoS policy named **downlink**.

```
[PE2] qos policy downlink
```

   # Associate class **downlink100** with behavior **remark_to_10**.

```
[PE2-qospolicy-downlink] classifier downlink100 behavior remark_to_10
```

Associate class **downlink200** with behavior **remark_to_20**.

```
[PE2-qospolicy-downlink] classifier downlink200 behavior remark_to_20
[PE2-qospolicy-downlink] quit
```

4. Configure the customer-side port GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type hybrid
```

Configure GigabitEthernet 1/0/1 to permit the packets from VLANs 10, 20, 100, and 200 to pass through tagged.

```
[PE2-GigabitEthernet1/0/1] port hybrid vlan 10 20 100 200 tagged
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[PE2-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Enable basic QinQ on GigabitEthernet 1/0/1.

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

Apply the policy named **uplink** to the incoming traffic of GigabitEthernet 1/0/1.

```
[PE2-GigabitEthernet1/0/1] qos apply policy uplink inbound
```

Apply the policy named **downlink** to the outgoing traffic of GigabitEthernet 1/0/1.

```
[PE2-GigabitEthernet1/0/1] qos apply policy downlink outbound
[PE2-GigabitEthernet1/0/1] quit
```

5. Configure the network-side port GigabitEthernet 1/0/2:

Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLANs 100 and 200.

```
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[PE2-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE2-GigabitEthernet1/0/2] quit
```

Configuring other devices in the service provider network

Configure all ports on the path between PE 1 and PE 2 to allow frames from VLANs 100 and 200 to pass through without removing the SVLAN tags.

Verifying the configuration

This example uses GigabitEthernet 1/0/1 on PE 1 to verify the configuration.

Display the port configurations.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1]display this
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 20 100 200 tagged
 qinq enable
```

```
 qos apply policy uplink inbound
 qos apply policy downlink outbound
#
return
```

Check whether the policies have been successfully applied to the port.

```
[PE1]display qos policy interface GigabitEthernet 1/0/1

  Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: uplink
   Classifier: uplink10
     Operator: AND
     Rule(s) : If-match customer-vlan-id 10
     Behavior: remark_to_100
      Marking:
        Remark Service VLAN ID 100
   Classifier: uplink20
     Operator: AND
     Rule(s) : If-match customer-vlan-id 20
     Behavior: remark_to_200
      Marking:
        Remark Service VLAN ID 200

  Direction: Outbound

  Policy: downlink
   Classifier: downlink100
     Operator: AND
     Rule(s) : If-match service-vlan-id 100
     Behavior: remark_to_10
      Marking:
        Remark Customer VLAN ID 10
   Classifier: downlink200
     Operator: AND
     Rule(s) : If-match service-vlan-id 200
     Behavior: remark_to_20
      Marking:
        Remark Customer VLAN ID 20
```

Configuration files

- PE 1:

```
#
vlan 10
#
vlan 20
```

```
#
vlan 100
#
vlan 200
#
traffic classifier uplink10 operator and
 if-match customer-vlan-id 10
traffic classifier uplink20 operator and
 if-match customer-vlan-id 20
traffic classifier downlink100 operator and
 if-match service-vlan-id 100
traffic classifier downlink200 operator and
 if-match service-vlan-id 200
#
traffic behavior remark_to_100
 remark service-vlan-id 100
traffic behavior remark_to_200
 remark service-vlan-id 200
traffic behavior remark_to_10
 remark customer-vlan-id 10
traffic behavior remark_to_20
 remark customer-vlan-id 20
#
qos policy uplink
 classifier uplink10 behavior remark_to_100
 classifier uplink20 behavior remark_to_200
qos policy downlink
 classifier downlink100 behavior remark_to_10
 classifier downlink200 behavior remark_to_20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 20 100 200 tagged
 qinq enable
 qos apply policy uplink inbound
 qos apply policy downlink outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

- PE 2:

```
#
vlan 10
```

```
#
vlan 20
#
vlan 100
#
vlan 200
#
traffic classifier uplink10 operator and
 if-match customer-vlan-id 10
traffic classifier uplink20 operator and
 if-match customer-vlan-id 20
traffic classifier downlink100 operator and
 if-match service-vlan-id 100
traffic classifier downlink200 operator and
 if-match service-vlan-id 200
#
traffic behavior remark_to_100
 remark service-vlan-id 100
traffic behavior remark_to_200
 remark service-vlan-id 200
traffic behavior remark_to_10
 remark customer-vlan-id 10
traffic behavior remark_to_20
 remark customer-vlan-id 20
#
qos policy uplink
 classifier uplink10 behavior remark_to_100
 classifier uplink20 behavior remark_to_200
qos policy downlink
 classifier downlink100 behavior remark_to_10
 classifier downlink200 behavior remark_to_20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 20 100 200 tagged
 qinq enable
 qos apply policy uplink inbound
 qos apply policy downlink outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

Example: Configuring two-to-two VLAN mapping

Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

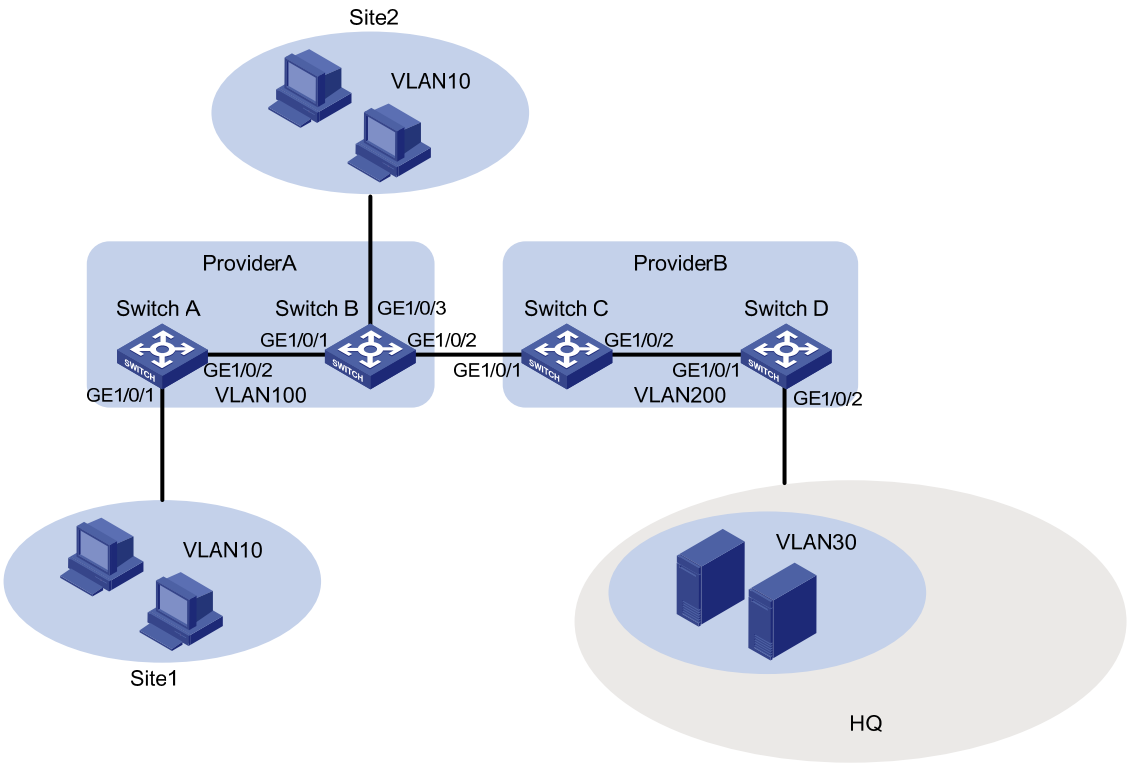
Network requirements

As shown in Figure 241:

- Site 1 and Site 2 are two branches of a company, and they both belong to VLAN 10. The two branches communicate with each other through a QinQ tunnel over service provider A's network. Service provider A allocates SVLAN 100 to the company.
- After the company is acquired by another company, the two sites must access the network of the new company.
- The VPN service of the new company is provided by service provider B, which allocates SVLAN 200 to the new company.
- The headquarters of the new company uses VLAN 30 to provide services for the two sites.

Configure two-to-two VLAN mapping, so that the two sites can access VLAN 30 in the headquarters without changing the VLAN configurations for the sites and SVLANs.

Figure 241 Network diagram



Configuration restrictions and guidelines

You need to configure two-to-two VLAN mapping on only one of the edge devices connecting the two service provider networks. This example uses Switch C.

Configuration procedures

Configuring Switch A

Create VLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
```

Configure QinQ on GigabitEthernet 1/0/1 to add outer VLAN tag 100 to packets from VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port access vlan 100
[SwitchA-GigabitEthernet1/0/1] qinq enable
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLAN 100.

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B

Create VLAN 100.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit
```

Configure QinQ on GigabitEthernet 1/0/3 to add outer VLAN tag 100 to packets from VLAN 10.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port access vlan 100
[SwitchB-GigabitEthernet1/0/3] qinq enable
[SwitchB-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to VLAN 100.

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLAN 100.

```
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/2] quit
```

Configuring Switch C

1. Create SVLAN 200.

   ```
   <SwitchC> system-view
   [SwitchC] vlan 200
   [SwitchC-vlan200] quit
   ```

2. Configure VLAN mapping for the traffic received on GigabitEthernet 1/0/1:

   # Configure a class named **uplink_in** to match traffic with inner VLAN tag 10 and outer VLAN tag 100.

   ```
   [SwitchC] traffic classifier uplink_in
   [SwitchC-classifier-uplink_in] if-match customer-vlan-id 10
   [SwitchC-classifier-uplink_in] if-match service-vlan-id 100
   [SwitchC-classifier-uplink_in] quit
   ```

   # Configure a behavior named **uplink_in** to change the outer VLAN tag into VLAN tag 200.

```
[SwitchC] traffic behavior uplink_in
[SwitchC-behavior-uplink_in] remark service-vlan-id 200
[SwitchC-behavior-uplink_in] quit
```

Create a QoS policy named **uplink_in**.

```
[SwitchC] qos policy uplink_in
```

Associate class **uplink_in** with traffic behavior **uplink_in** in the QoS policy.

```
[SwitchC-qospolicy-uplink_in] classifier uplink_in behavior uplink_in
[SwitchC-qospolicy-uplink_in] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to VLAN 200.

```
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 200
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Apply QoS policy **uplink_in** to the incoming traffic of GigabitEthernet 1/0/1.

```
[SwitchC-GigabitEthernet1/0/1] qos apply policy uplink_in inbound
[SwitchC-GigabitEthernet1/0/1] quit
```

3. Configure VLAN mapping for the traffic sent out of GigabitEthernet 1/0/2:

Configure a class named **uplink_out** to match traffic with inner VLAN tag 10 and outer VLAN tag 200.

```
[SwitchC] traffic classifier uplink_out
[SwitchC-classifier-uplink_out] if-match customer-vlan-id 10
[SwitchC-classifier-uplink_out] if-match service-vlan-id 200
[SwitchC-classifier-uplink_out] quit
```

Configure a behavior named **uplink_out** to change the inner VLAN tag into VLAN tag 30.

```
[SwitchC] traffic behavior uplink_out
[SwitchC-behavior-uplink_out] remark customer-vlan-id 30
[SwitchC-behavior-uplink_out] quit
```

Create a QoS policy named **uplink_out**.

```
[SwitchC] qos policy uplink_out
```

Associate class **uplink_out** with traffic behavior **uplink_out** in the QoS policy.

```
[SwitchC-qospolicy-uplink_out] classifier uplink_out behavior uplink_out
[SwitchC-qospolicy-uplink_out] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLAN 200.

```
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 200
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

Apply QoS policy **uplink_out** to the outgoing traffic of GigabitEthernet 1/0/2.

```
[SwitchC-GigabitEthernet1/0/2] qos apply policy uplink_out outbound
[SwitchC-GigabitEthernet1/0/2] quit
```

4. Configure VLAN mapping for the traffic sent out of GigabitEthernet 1/0/1:

Configure a class named **downlink_out** to match traffic with inner VLAN tag 30 and outer VLAN tag 200.

```
[SwitchC] traffic classifier downlink_out
[SwitchC-classifier-downlink_out] if-match customer-vlan-id 30
[SwitchC-classifier-downlink_out] if-match service-vlan-id 200
[SwitchC-classifier-downlink_out] quit
```

Configure a behavior named **downlink_out** to change the inner VLAN tag into VLAN tag 10 and change the outer VLAN tag into VLAN tag 100.

```
[SwitchC] traffic behavior downlink_out
[SwitchC-behavior-downlink_out] remark customer-vlan-id 10
[SwitchC-behavior-downlink_out] remark service-vlan-id 100
[SwitchC-behavior-downlink_out] quit
```

Create a QoS policy named **downlink_out**.

```
[SwitchC] qos policy downlink_out
```

Associate class **downlink_out** with traffic behavior **downlink_out** in the QoS policy.

```
[SwitchC-qospolicy-downlink_out] classifier downlink_out behavior downlink_out
[SwitchC-qospolicy-downlink_out] quit
```

Apply QoS policy **downlink_out** to the outgoing traffic of GigabitEthernet 1/0/1.

```
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] qos apply policy downlink_out outbound
[SwitchC-GigabitEthernet1/0/1] quit
```

Configuring Switch D

Create VLAN 200.

```
<SwitchD> system-view
[SwitchD] vlan 200
[SwitchD-vlan200] quit
```

Configure QinQ on GigabitEthernet 1/0/2 to add outer VLAN tag 200 to packets from VLAN 30.

```
[SwitchD] interface gigabitethernet 1/0/2
[SwitchD-GigabitEthernet1/0/2] port access vlan 200
[SwitchD-GigabitEthernet1/0/2] qinq enable
[SwitchD-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to VLAN 200.

```
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 200
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchD-GigabitEthernet1/0/1] quit
```

Verifying the configuration

This example uses GigabitEthernet 1/0/1 on Switch C to verify the configuration.

Display the port configurations.

```
[SwitchC] interface gigabitethernet 1/0/1
```

```
[SwitchC-GigabitEthernet1/0/1]display this
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
 qos apply policy uplink_in inbound
 qos apply policy downlink_out outbound
#
return
```

Display the QoS policies applied to the port.

```
[SwitchC]display qos policy interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: uplink_in
   Classifier: uplink_in
     Operator: AND
     Rule(s) : If-match customer-vlan-id 10
               If-match service-vlan-id 100
     Behavior: uplink_in
      Marking:
        Remark Service VLAN ID 200

  Direction: Outbound

  Policy: downlink_out
   Classifier: downlink_out
     Operator: AND
     Rule(s) : If-match customer-vlan-id 30
               If-match service-vlan-id 200
     Behavior: downlink_out
      Marking:
        Remark Customer VLAN ID 10
      Marking:
        Remark Service VLAN ID 100
```

Display the QoS policies applied to the port.

```
[SwitchC]display qos policy interface GigabitEthernet 1/0/2

  Interface: GigabitEthernet1/0/2

  Direction: Outbound

  Policy: uplink_out
   Classifier: uplink_out
     Operator: AND
     Rule(s) : If-match customer-vlan-id 10
               If-match service-vlan-id 200
```

```
Behavior: uplink_out
 Marking:
   Remark Customer VLAN ID 30
```

Configuration files

- Switch A:

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port access vlan 100
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
```

- Switch B:

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 qinq enable
```

- Switch C:

```
#
vlan 200
#
traffic classifier uplink_in operator and
 if-match customer-vlan-id 10
 if-match service-vlan-id 100
traffic classifier uplink_out operator and
 if-match customer-vlan-id 10
 if-match service-vlan-id 200
traffic classifier downlink_out operator and
 if-match customer-vlan-id 30
```

```
 if-match service-vlan-id 200
#
traffic behavior uplink_in
 remark service-vlan-id 200
traffic behavior uplink_out
 remark customer-vlan-id 30
traffic behavior downlink_out
 remark customer-vlan-id 10
 remark service-vlan-id 100
#
qos policy uplink_in
 classifier uplink_in behavior uplink_in
qos policy uplink_out
 classifier uplink_out behavior uplink_out
qos policy downlink_out
 classifier downlink_out behavior downlink_out
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
 qos apply policy uplink_in inbound
 qos apply policy downlink_out outbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
 qos apply policy uplink_out outbound
```

- Switch D:

```
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
#
interface GigabitEthernet1/0/2
 port access vlan 200
 qinq enable
```

VPLS configuration examples

This document provides VPLS configuration examples.

Virtual Private LAN Service (VPLS) delivers point-to-multipoint L2VPN services over an MPLS or IP backbone. The provider backbone emulates a switch to connect all geographically dispersed sites for each customer network. The backbone is transparent to the customer sites, which can communicate with each other as if they were on the same LAN.

VPLS has two networking models: full mesh and H-VPLS.

The full mesh model supports the following signaling protocols:

- **LDP**—Applies to the scenario where a few sites exist and no new sites will be added.
- **BGP**—Applies to the scenario where a lot of sites exist and new sites will be added.

The H-VPLS model supports the following access modes:

- **LSP access**—Applies to the scenario where the devices connected to customer sites support MPLS. In this mode, customer packets directly enter the LSP tunnel.
- **QinQ access**—Applies to the scenario where the devices connected to customer sites do not support MPLS. In this mode, customer packets are added with an outer VLAN tag before they enter the LSP tunnel.

General configuration restrictions and guidelines

Hardware requirements

To support VPLS, the HP 7500 Switch Series must use an EB, SD, LSQ1QGS4SC, or LSQ1QGC4SC card, and use the ports on the card to connect to the user network and carrier network.

Example: Configuring full-mesh VPLS using LDP

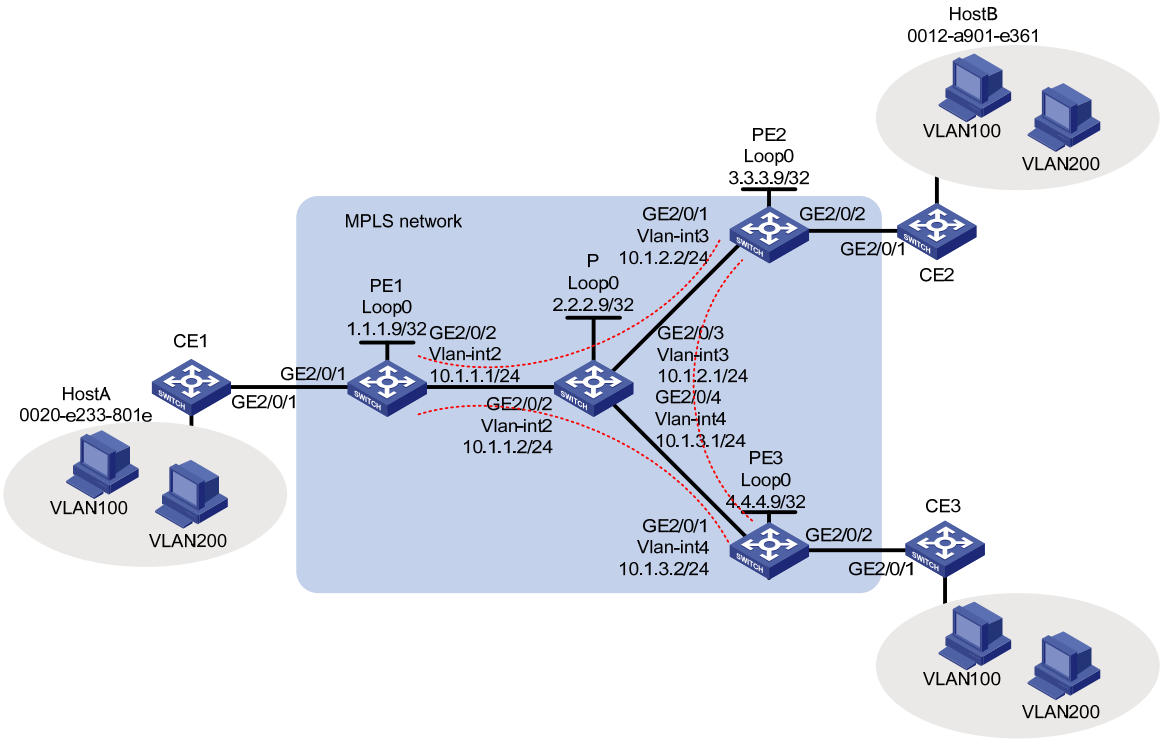
Applicable product matrix

Product series	Software version
HP 7500	Release series 6620
	Release series 6630
	Release series 6700

Network requirements

As shown in Figure 242, a customer has three branches that connect to an MPLS backbone through CE 1, CE 2, and CE 3, respectively. Configure full-mesh VPLS using LDP so the three branches can communicate with each other at Layer 2.

Figure 242 Network diagram



Requirements analysis

To negotiate inner labels, configure any two PEs as LDP peers.

To identify packets to be transported by VPLS, configure service instances on the AC ports of PEs.

To retain the VLAN information for each site, configure the AC access mode as Ethernet and the VPLS instance encapsulation mode as Ethernet on the AC ports of PEs.

Configuration procedures

Configuring CE 1

1. Configure CE 1 as follows:

   # Create VLAN 100 and VLAN 200.

   ```
   <CE1> system-view
   [CE1] vlan 100
   [CE1-vlan100] quit
   [CE1] vlan 200
   [CE1-vlan200] quit
   ```

   # Configure the uplink port GigabitEthernet 2/0/1 as a trunk port.

   ```
   [CE1] interface GigabitEthernet 2/0/1
   [CE1-GigabitEthernet2/0/1] port link-type trunk
   ```

   # Configure the port to permit packets of VLAN 100 and VLAN 200 to pass with VLAN tags.

   ```
   [CE1-GigabitEthernet2/0/1] port trunk permit vlan 100 200
   ```

2. Configure CE 2 and CE 3 in the same way that CE 1 is configured. (Details not shown.)

Configuring PE 1

1. Configure MPLS and LDP to establish public LSPs:

   # Configure the LSR ID, and enable MPLS globally.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
```

   # Enable MPLS L2VPN and MPLS LDP globally.

```
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] l2vpn
[PE1-l2vpn] mpls l2vpn
[PE1-l2vpn] quit
```

   # Create VLAN 2, and add GigabitEthernet 2/0/2 to VLAN 2.

```
[PE1] vlan 2
[PE1-vlan2] port GigabitEthernet 2/0/2
[PE1-vlan2] quit
```

   # Create VLAN-interface 2, configure an IP address for the interface, and enable MPLS and MPLS LDP on the interface.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

   # Configure OSPF for LSP establishment.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

2. Create a VPLS instance and configure the remote LDP peers:

   # Establish a remote LDP session to PE 2.

```
[PE1] mpls ldp remote-peer 1
[PE1-mpls-ldp-remote-1] remote-ip 3.3.3.9
[PE1-mpls-ldp-remote-1] quit
```

   # Establish a remote LDP session to PE 3.

```
[PE1] mpls ldp remote-peer 2
[PE1-mpls-ldp-remote-2] remote-ip 4.4.4.9
[PE1-mpls-ldp-remote-2] quit
```

   # Create a VPLS instance named **user_a** and configure the encapsulation mode as **Ethernet**.

```
[PE1] vsi user_a static
[PE1-vsi-user_a] encapsulation ethernet
```

Configure the signaling protocol as LDP.

```
[PE1-vsi-user_a] pwsignal ldp
```

Set the VSI ID of the VPLS instance to 500. The VSI ID must be unique on the MPLS network.

```
[PE1-vsi-user_a-ldp] vsi-id 500
```

Configure PE 2 and PE 3 as the remote LDP peers of PE 1.

```
[PE1-vsi-user_a-ldp] peer 3.3.3.9
[PE1-vsi-user_a-ldp] peer 4.4.4.9
[PE1-vsi-user_a-ldp] quit
[PE1-vsi-user_a] quit
```

3. Create service instances on the downlink port GigabitEthernet 2/0/1 and bind the service instances to the VPLS instance:

Configure service instance 100: match VLAN 100, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] service-instance 100
[PE1-GigabitEthernet2/0/1-srv100] encapsulation s-vid 100
[PE1-GigabitEthernet2/0/1-srv100] xconnect vsi user_a access-mode ethernet
[PE1-GigabitEthernet2/0/1-srv100] quit
```

Configure service instance 200: match VLAN 200, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE1-GigabitEthernet2/0/1] service-instance 200
[PE1-GigabitEthernet2/0/1-srv200] encapsulation s-vid 200
[PE1-GigabitEthernet2/0/1-srv200] xconnect vsi user_a access-mode ethernet
[PE1-GigabitEthernet2/0/1-srv200] quit
[PE1-GigabitEthernet2/0/1] quit
```

Configuring PE 2

1. Configure MPLS and LDP to establish public LSPs:

Configure the LSR ID, and enable MPLS globally.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
```

Enable MPLS L2VPN and MPLS LDP globally.

```
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] l2vpn
[PE2-l2vpn] mpls l2vpn
[PE2-l2vpn] quit
```

Create VLAN 3, and add GigabitEthernet 2/0/1 to VLAN 3.

```
[PE2] vlan 3
```

```
[PE2-vlan3] port GigabitEthernet 2/0/1
[PE2-vlan3] quit
```

Create VLAN-interface 3, configure an IP address for the interface, and enable MPLS and MPLS LDP on the interface.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

Configure OSPF for LSP establishment.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

2. Create a VPLS instance, and configure the remote LDP peers:

Establish a remote LDP session to PE 1.

```
[PE2] mpls ldp remote-peer 1
[PE2-mpls-ldp-remote-1] remote-ip 1.1.1.9
[PE2-mpls-ldp-remote-1] quit
```

Establish a remote LDP session to PE 3.

```
[PE2] mpls ldp remote-peer 2
[PE2-mpls-ldp-remote-2] remote-ip 4.4.4.9
[PE2-mpls-ldp-remote-2] quit
```

Create a VPLS instance named **user_a** and configure the encapsulation mode as **Ethernet**.

```
[PE2] vsi user_a static
[PE2-vsi-user_a] encapsulation ethernet
```

Configure the signaling protocol as LDP.

```
[PE2-vsi-user_a] pwsignal ldp
```

Set the VSI ID of the VPLS instance to 500. The VSI ID must be the same as that configured on PE 1.

```
[PE2-vsi-user_a-ldp] vsi-id 500
```

Configure PE 1 and PE 3 as the remote LDP peers of PE 2.

```
[PE2-vsi-user_a-ldp] peer 1.1.1.9
[PE2-vsi-user_a-ldp] peer 4.4.4.9
[PE2-vsi-user_a-ldp] quit
[PE2-vsi-user_a] quit
```

3. Create service instances on the downlink port GigabitEthernet 2/0/2 and bind the service instances to the VPLS instance:

Configure service instance 100: match VLAN 100, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] service-instance 100
[PE2-GigabitEthernet2/0/2-srv100] encapsulation s-vid 100
[PE2-GigabitEthernet2/0/2-srv100] xconnect vsi user_a access-mode ethernet
```

```
[PE2-GigabitEthernet2/0/2-srv100] quit
```

Configure service instance 200: match VLAN 200, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE2-GigabitEthernet2/0/2] service-instance 200
[PE2-GigabitEthernet2/0/2-srv200] encapsulation s-vid 200
[PE2-GigabitEthernet2/0/2-srv200] xconnect vsi user_a access-mode ethernet
[PE2-GigabitEthernet2/0/2-srv200] quit
[PE2-GigabitEthernet2/0/2] quit
```

Configuring PE 3

1. Configure MPLS and LDP to establish public LSPs:

Configure the LSR ID, and enable MPLS globally.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 4.4.4.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 4.4.4.9
[PE3] mpls
[PE3-mpls] lsp-trigger all
[PE3-mpls] quit
```

Enable MPLS L2VPN and MPLS LDP globally.

```
[PE3] mpls ldp
[PE3-mpls-ldp] quit
[PE3] l2vpn
[PE3-l2vpn] mpls l2vpn
[PE3-l2vpn] quit
```

Create VLAN 4, and add GigabitEthernet 2/0/1 to VLAN 4.

```
[PE3] vlan 4
[PE3-vlan4] port GigabitEthernet 2/0/1
[PE3-vlan4] quit
```

Create VLAN-interface 4, configure an IP address for the interface, and enable MPLS and MPLS LDP on the interface.

```
[PE2] interface vlan-interface 4
[PE2-Vlan-interface4] ip address 10.1.3.2 24
[PE2-Vlan-interface4] mpls
[PE2-Vlan-interface4] mpls ldp
[PE2-Vlan-interface4] quit
```

Configure OSPF for LSP establishment.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

2. Create a VPLS instance and configure the remote LDP peers:

Establish a remote LDP session to PE 1.

```
[PE3] mpls ldp remote-peer 1
```

```
[PE3-mpls-ldp-remote-1] remote-ip 1.1.1.9
[PE3-mpls-ldp-remote-1] quit
```

Establish a remote LDP session to PE 2.

```
[PE3] mpls ldp remote-peer 2
[PE3-mpls-ldp-remote-2] remote-ip 3.3.3.9
[PE3-mpls-ldp-remote-2] quit
```

Create a VPLS instance named **user_a** and configure the encapsulation mode as **Ethernet**.

```
[PE3] vsi user_a static
[PE3-vsi-user_a] encapsulation ethernet
```

Configure the signaling protocol as LDP.

```
[PE3-vsi-user_a] pwsignal ldp
```

Set the VSI ID of the VPLS instance to 500. The VSI ID must be the same as that configured on PE 1.

```
[PE3-vsi-user_a-ldp] vsi-id 500
```

Configure PE 1 and PE 2 as the remote LDP peers of PE 3.

```
[PE3-vsi-user_a-ldp] peer 1.1.1.9
[PE3-vsi-user_a-ldp] peer 3.3.3.9
[PE3-vsi-user_a-ldp] quit
[PE3-vsi-user_a] quit
```

3. Create service instances on the downlink port GigabitEthernet 2/0/2 and bind the service instances to the VPLS instance:

   # Configure service instance 100: match VLAN 100, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE3] interface gigabitethernet 2/0/2
[PE3-GigabitEthernet2/0/2] service-instance 100
[PE3-GigabitEthernet2/0/2-srv100] encapsulation s-vid 100
[PE3-GigabitEthernet2/0/2-srv100] xconnect vsi user_a access-mode ethernet
[PE3-GigabitEthernet2/0/2-srv100] quit
```

   # Configure service instance 200: match VLAN 200, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE3-GigabitEthernet2/0/2] service-instance 200
[PE3-GigabitEthernet2/0/2-srv200] encapsulation s-vid 200
[PE3-GigabitEthernet2/0/2-srv200] xconnect vsi user_a access-mode ethernet
[PE3-GigabitEthernet2/0/2-srv200] quit
[PE3-GigabitEthernet2/0/2] quit
```

Configuring the P device

1. Configure a loopback interface and its IP address.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
```

2. Configure the LSR ID, and enable MPLS globally.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] lsp-trigger all
[P-mpls] quit
```

3. Enable LDP globally.

```
[P] mpls ldp
[P-mpls-ldp] quit
```

4. Configure VLAN-interface 2 that connects to PE 1, and enable LDP on the interface.

```
[P] vlan 2
[P-vlan2] port access gigabitethernet 2/0/2
[P-vlan2] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
```

5. Configure VLAN-interface 3 that connects to PE 2, and enable LDP on the interface.

```
[P] vlan 3
[P-vlan3] port access gigabitethernet 2/0/3
[P-vlan3] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

6. Configure VLAN-interface 4 that connects to PE 3, and enable LDP on the interface.

```
[P] vlan 4
[P-vlan4] port access gigabitethernet 2/0/4
[P-vlan4] quit
[P] interface vlan-interface 4
[P-Vlan-interface4] ip address 10.1.3.1 24
[P-Vlan-interface4] mpls
[P-Vlan-interface4] mpls ldp
[P-Vlan-interface4] quit
```

7. Configure OSPF for LSP establishment.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Verifying the configuration

Checking public LSPs

Execute the **display mpls ldp lsp** command on each device to view the LDP LSP information. This example uses PE 1.

```
<PE1> display mpls ldp lsp
                                LDP LSP Information
```

```
------------------------------------------------------------------------
SN  DestAddress/Mask   In/OutLabel   Next-Hop     In/Out-Interface
------------------------------------------------------------------------
1    1.1.1.9/32         3/NULL       127.0.0.1     Vlan2/InLoop0
2    2.2.2.9/32         NULL/3       10.1.1.2      ----/Vlan2
3    3.3.3.9/32         NULL/1025    10.1.1.2      ----/Vlan2
4    4.4.4.9/32         NULL/1026    10.1.1.2      ----/Vlan2
5    10.1.2.0/24        NULL/3       10.1.1.2      ----/Vlan2
6    10.1.3.0/24        NULL/3       10.1.1.2      ----/Vlan2
------------------------------------------------------------------------
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

Checking PW connections

Execute the **display vpls connection** command on each PE. The output shows that PW connections in up state have been established. This example uses PE 1.

```
<PE1> display vpls connection vsi user_a verbose
VSI Name: user_a                                Signaling: ldp
  **Remote Vsi ID   : 500
    VC State        : up
    Encapsulation   : vlan
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 3.3.3.9
    PW Type         : label
    Local VC Label  : 89766
    Remote VC Label : 81922
    Link ID         : 1
    Tunnel Policy   : --
    Tunnel ID       : 0x4600068
VSI Name: user_a                                Signaling: ldp
  **Remote Vsi ID   : 500
    VC State        : up
    Encapsulation   : vlan
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 4.4.4.9
    PW Type         : label
    Local VC Label  : 89767
    Remote VC Label : 81973
    Link ID         : 1
    Tunnel Policy   : --
    Tunnel ID       : 0x4600069
```

Configuration files

- PE 1:

  ```
  #
  ```

```
 mpls lsr-id 1.1.1.9
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.9
#
mpls ldp remote-peer 2
 remote-ip 4.4.4.9
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 3.3.3.9
  peer 4.4.4.9
 encapsulation ethernet
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a access-mode ethernet
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_a access-mode ethernet
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
```

- PE 2:

```
#
```

```
 mpls lsr-id 3.3.3.9
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 1.1.1.9
#
mpls ldp remote-peer 2
 remote-ip 4.4.4.9
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 1.1.1.9
  peer 4.4.4.9
 encapsulation ethernet
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port access vlan 3
#
interface GigabitEthernet2/0/2
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a access-mode ethernet
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_a access-mode ethernet
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
```

- PE 3:

```
#
```

```
 mpls lsr-id 4.4.4.9
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 1.1.1.9
#
mpls ldp remote-peer 2
 remote-ip 3.3.3.9
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 1.1.1.9
  peer 3.3.3.9
 encapsulation ethernet
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
interface Vlan-interface4
 ip address 10.1.3.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port access vlan 4
#
interface GigabitEthernet2/0/2
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a access-mode ethernet
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_a access-mode ethernet
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 4.4.4.9 0.0.0.0
```

- P:

```
#
```

```
 mpls lsr-id 2.2.2.9
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface4
 ip address 10.1.3.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
interface GigabitEthernet2/0/3
 port access vlan 3
#
interface GigabitEthernet2/0/4
 port access vlan 4
#
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
  network 10.1.3.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
```

Example: Configuring full-mesh VPLS using BGP

Applicable product matrix

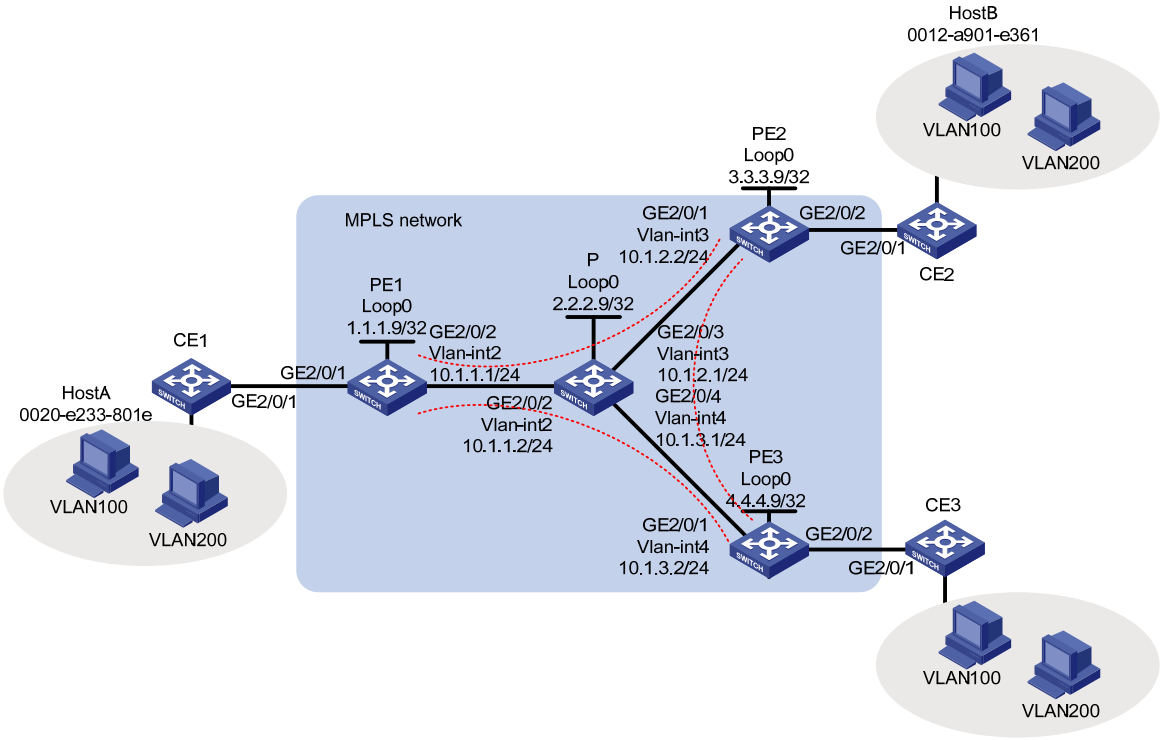
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 243, a customer has three branches that connect to an MPLS backbone through CE 1, CE 2, and CE 3, respectively, and the customer will add sites.

Configure full-mesh VPLS using BGP so the three branches can communicate with each other at Layer 2.

Figure 243 Network diagram



Requirements analysis

To identify a VPLS instance, configure RD and route target attributes on PEs.

To identify packets to be transported by VPLS, configure service instances and match criteria on the AC ports of PEs.

To retain the VLAN information for each site, configure the AC access mode as Ethernet and the VPLS instance encapsulation mode as Ethernet on the AC ports of PEs.

Configuration procedures

Configuring CE 1

1. Configure CE 1 as follows:

   # Create VLAN 100 and VLAN 200.

   ```
   <CE1> system-view
   [CE1] vlan 100
   [CE1-vlan100] quit
   [CE1] vlan 200
   [CE1-vlan200] quit
   ```

   # Configure the uplink port GigabitEthernet 2/0/1 as a trunk port.

   ```
   [CE1] interface GigabitEthernet 2/0/1
   [CE1-GigabitEthernet2/0/1] port link-type trunk
   ```

   Configure the port to permit packets of VLAN 100 and VLAN 200 to pass with VLAN tags.

   ```
   [CE1-GigabitEthernet2/0/1] port trunk permit vlan 100 200
   ```

2. Configure CE 2 and CE 3 in the same way that CE 1 is configured. (Details not shown.)

Configuring PE 1

1. Configure MPLS and LDP to establish public LSPs:

   # Configure the LSR ID, and enable MPLS globally.

   ```
   <PE1> system-view
   [PE1] interface loopback 0
   [PE1-LoopBack0] ip address 1.1.1.9 32
   [PE1-LoopBack0] quit
   [PE1] mpls lsr-id 1.1.1.9
   [PE1] mpls
   [PE1-mpls] lsp-trigger all
   [PE1-mpls] quit
   ```

   # Enable MPLS L2VPN and LDP globally.

   ```
   [PE1] mpls ldp
   [PE1-mpls-ldp] quit
   [PE1] l2vpn
   [PE1-l2vpn] mpls l2vpn
   [PE1-l2vpn] quit
   ```

   # Create VLAN 2, and add GigabitEthernet 2/0/2 to VLAN 2.

   ```
   [PE1] vlan 2
   [PE1-vlan2] port GigabitEthernet 2/0/2
   [PE1-vlan2] quit
   ```

   # Create VLAN-interface 2, configure an IP address for the interface, and enable MPLS and MPLS LDP on the interface.

   ```
   [PE1] interface vlan-interface 2
   [PE1-Vlan-interface2] ip address 10.1.1.1 24
   [PE1-Vlan-interface2] mpls
   [PE1-Vlan-interface2] mpls ldp
   [PE1-Vlan-interface2] quit
   ```

   # Configure OSPF for LSP establishment.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

2. Configure BGP extensions and create VPLS address family peers for PE 1:

   # Enable BGP process 100, and configure PE 2 and PE 3 as the peers of PE 1.

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 4.4.4.9 as-number 100
```

   # Configure the source interface for TCP connections to the peers as loopback interface 0.

```
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] peer 4.4.4.9 connect-interface loopback 0
```

   # Enter VPLS address family view, and enable peers PE 2 and PE 3.

```
[PE1-bgp] vpls-family
[PE1-bgp-af-vpls] peer 3.3.3.9 enable
[PE1-bgp-af-vpls] peer 4.4.4.9 enable
[PE1-bgp-af-vpls] quit
[PE1-bgp] quit
```

   # Create a VPLS instance named **user_a** and configure the encapsulation mode as **Ethernet**.

```
[PE1] vsi user_a auto
[PE1-vsi-user_a] encapsulation ethernet
```

   # Configure the signaling protocol as BGP.

```
[PE1-vsi-user_a] pwsignal bgp
```

   # Configure a route distinguisher and route target for the VPLS instance.

```
[PE1-vsi-bbb-bgp] route-distinguisher 100:1
[PE1-vsi-bbb-bgp] vpn-target 111:1
```

   # Configure the site number of PE 1 in the VPLS instance as 1. Specify the maximum number of sites in the VPLS instance as 12.

```
[PE1-vsi-bbb-bgp] site 1 range 12
[PE1-vsi-bbb] quit
```

3. Create service instances on the downlink port GigabitEthernet 2/0/1 and bind the service instances to the VPLS instance:

   # Configure service instance 100: match VLAN 100, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE1] interface gigabitethernet 2/0/1
[PE1-GigabitEthernet2/0/1] service-instance 100
[PE1-GigabitEthernet2/0/1-srv100] encapsulation s-vid 100
[PE1-GigabitEthernet2/0/1-srv100] xconnect vsi user_a access-mode ethernet
[PE1-GigabitEthernet2/0/1-srv100] quit
```

   # Configure service instance 200: match VLAN 200, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE1-GigabitEthernet2/0/1] service-instance 200
[PE1-GigabitEthernet2/0/1-srv200] encapsulation s-vid 200
[PE1-GigabitEthernet2/0/1-srv200] xconnect vsi user_a access-mode ethernet
```

```
[PE1-GigabitEthernet2/0/1-srv200] quit
[PE1-GigabitEthernet2/0/1] quit
```

Configuring PE 2

1. Configure MPLS and LDP to establish public LSPs:

   # Configure the LSR ID, and enable MPLS globally.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
```

   # Enable MPLS L2VPN and MPLS LDP globally.

```
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] l2vpn
[PE2-l2vpn] mpls l2vpn
[PE2-l2vpn] quit
```

   # Create VLAN 3, and add GigabitEthernet 2/0/1 to VLAN 3.

```
[PE2] vlan 3
[PE2-vlan3] port GigabitEthernet 2/0/1
[PE2-vlan3] quit
```

   # Create VLAN-interface 3, configure an IP address for the interface, and enable MPLS and MPLS LDP on the interface.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] mpls ldp
[PE2-Vlan-interface3] quit
```

   # Configure OSPF for LSP establishment.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

2. Configure BGP extensions and create VPLS address family peers for PE 2:

   # Enable BGP process 100, and configure PE 1 and PE 3 as the peers of PE 2.

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 4.4.4.9 as-number 100
```

   # Configure the source interface for TCP connections to the peers as loopback interface 0.

```
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
```

   # Enter VPLS address family view, and enable peers PE 1 and PE 3.

```
[PE2-bgp] vpls-family
```

```
[PE2-bgp-af-vpls] peer 1.1.1.9 enable
[PE2-bgp-af-vpls] peer 4.4.4.9 enable
[PE2-bgp-af-vpls] quit
[PE2-bgp] quit
```

Create a VPLS instance named **user_a** and configure the encapsulation mode as **Ethernet**.

```
[PE2] vsi user_a auto
[PE2-vsi-user_a] encapsulation ethernet
```

Configure the signaling protocol as BGP.

```
[PE2-vsi-user_a] pwsignal bgp
```

Configure the same route distinguisher and route target for the VPLS instance as those configured on PE 1.

```
[PE2-vsi-bbb-bgp] route-distinguisher 100:1
[PE2-vsi-bbb-bgp] vpn-target 111:1
```

Set the site number of PE 2 in the VPLS instance to 2, and specify the maximum number of peer PEs as 12.

```
[PE2-vsi-bbb-bgp] site 2 range 12
[PE2-vsi-bbb] quit
```

3. Create service instances on the downlink port GigabitEthernet 2/0/2 and bind the service instances to the VPLS instance:

Configure service instance 100: match VLAN 100, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE2] interface gigabitethernet 2/0/2
[PE2-GigabitEthernet2/0/2] service-instance 100
[PE2-GigabitEthernet2/0/2-srv100] encapsulation s-vid 100
[PE2-GigabitEthernet2/0/2-srv100] xconnect vsi user_a access-mode ethernet
[PE2-GigabitEthernet2/0/2-srv100] quit
```

Configure service instance 200: match VLAN 200, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE2-GigabitEthernet2/0/2] service-instance 200
[PE2-GigabitEthernet2/0/2-srv200] encapsulation s-vid 200
[PE2-GigabitEthernet2/0/2-srv200] xconnect vsi user_a access-mode ethernet
[PE2-GigabitEthernet2/0/2-srv200] quit
[PE2-GigabitEthernet2/0/2] quit
```

Configuring PE 3

1. Configure MPLS and LDP to establish public LSPs:

Configure the LSR ID, and enable MPLS globally.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 4.4.4.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 4.4.4.9
[PE3] mpls
[PE3-mpls] quit
```

Enable MPLS L2VPN and MPLS LDP globally.

```
[PE3] mpls ldp
[PE3-mpls-ldp] quit
```

```
[PE3] l2vpn
[PE3-l2vpn] mpls l2vpn
[PE3-l2vpn] quit
```

Create VLAN 4, and add GigabitEthernet 2/0/1 to VLAN 4.

```
[PE3] vlan 4
[PE3-vlan4] port GigabitEthernet 2/0/1
[PE3-vlan4] quit
```

Create VLAN-interface 4, configure an IP address for the interface, and enable MPLS and MPLS LDP on the interface.

```
[PE2] interface vlan-interface 4
[PE2-Vlan-interface4] ip address 10.1.3.2 24
[PE2-Vlan-interface4] mpls
[PE2-Vlan-interface4] mpls ldp
[PE2-Vlan-interface4] quit
```

Configure OSPF for LSP establishment.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

2. Configure BGP extensions and create VPLS address family peers for PE 3:

Enable BGP process 100, and configure PE 1 and PE 2 as the BGP peers of PE 3.

```
[PE3] bgp 100
[PE3-bgp] peer 1.1.1.9 as-number 100
[PE3-bgp] peer 3.3.3.9 as-number 100
```

Configure the source interface for TCP connections to the peers as loopback interface 0.

```
[PE3-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE3-bgp] peer 3.3.3.9 connect-interface loopback 0
```

Enter VPLS address family view, and enable peers PE 1 and PE 2.

```
[PE3-bgp] vpls-family
[PE3-bgp-af-vpls] peer 1.1.1.9 enable
[PE3-bgp-af-vpls] peer 3.3.3.9 enable
[PE3-bgp-af-vpls] quit
[PE3-bgp] quit
```

Create a VPLS instance named **user_a** and configure the encapsulation mode as **Ethernet**.

```
[PE3] vsi user_a auto
[PE3-vsi-user_a] encapsulation ethernet
```

Configure the signaling protocol as BGP.

```
[PE3-vsi-user_a] pwsignal bgp
```

Configure the same route distinguisher and VPN target for the VPLS instance as those configured on PE 1.

```
[PE3-vsi-bbb-bgp] route-distinguisher 100:1
[PE3-vsi-bbb-bgp] vpn-target 111:1
```

Set the site number of PE 3 in the VPLS instance to 3, and specify the maximum number of peer PEs as 12.

```
[PE3-vsi-bbb-bgp] site 3 range 12
[PE3-vsi-bbb] quit
```

3. Create service instances on the downlink port GigabitEthernet 2/0/2 and bind the service instances to the VPLS instance:

   # Configure service instance 100: match VLAN 100, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE3] interface gigabitethernet 2/0/2
[PE3-GigabitEthernet2/0/2] service-instance 100
[PE3-GigabitEthernet2/0/2-srv100] encapsulation s-vid 100
[PE3-GigabitEthernet2/0/2-srv100] xconnect vsi user_a access-mode ethernet
[PE3-GigabitEthernet2/0/2-srv100] quit
```

   # Configure service instance 200: match VLAN 200, bind the instance to VPLS instance **user_a**, and enable Ethernet AC mode.

```
[PE3-GigabitEthernet2/0/2] service-instance 200
[PE3-GigabitEthernet2/0/2-srv200] encapsulation s-vid 200
[PE3-GigabitEthernet2/0/2-srv200] xconnect vsi user_a access-mode ethernet
[PE3-GigabitEthernet2/0/2-srv200] quit
[PE3-GigabitEthernet2/0/2] quit
```

Configuring the P device

1. Configure a loopback interface and its IP address.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
```

2. Configure the LSR ID, and enable MPLS globally.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
```

3. Enable LDP globally.

```
[P] mpls ldp
[P-mpls-ldp] quit
```

4. Configure VLAN-interface 2 that connects to PE 1, and enable LDP on the interface.

```
[P] vlan 2
[P-vlan2] port access gigabitethernet 2/0/2
[P-vlan2] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls
[P-Vlan-interface2] mpls ldp
[P-Vlan-interface2] quit
```

5. Configure VLAN-interface 3 that connects to PE 2, and enable LDP on the interface.

```
[P] vlan 3
[P-vlan3] port access gigabitethernet 2/0/3
[P-vlan3] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
```

```
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
```

6. Configure VLAN-interface 4 that connects to PE 3, and enable LDP on the interface.

```
[P] vlan 4
[P-vlan4] port access gigabitethernet 2/0/4
[P-vlan4] quit
[P] interface vlan-interface 4
[P-Vlan-interface4] ip address 10.1.3.1 24
[P-Vlan-interface4] mpls
[P-Vlan-interface4] mpls ldp
[P-Vlan-interface4] quit
```

7. Configure OSPF for LSP establishment.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Verifying the configuration

Checking public LSPs

Execute the **display mpls ldp lsp** command on each device to view the LDP LSP information. This example uses PE 1.

```
<PE1> display mpls ldp lsp
                              LDP LSP Information
 -------------------------------------------------------------------
 SN  DestAddress/Mask   In/OutLabel   Next-Hop     In/Out-Interface
 -------------------------------------------------------------------
 1    1.1.1.9/32         3/NULL       127.0.0.1     Vlan2/InLoop0
 2    2.2.2.9/32         NULL/3       10.1.1.2      ----/Vlan2
 3    3.3.3.9/32         NULL/1025    10.1.1.2      ----/Vlan2
 4    4.4.4.9/32         NULL/1026    10.1.1.2      ----/Vlan2
 5    10.1.2.0/24        NULL/3       10.1.1.2      ----/Vlan2
 6    10.1.3.0/24        NULL/3       10.1.1.2      ----/Vlan2
 -------------------------------------------------------------------
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
```

Checking PW connections

Execute the **display vpls connection** command on each PE. The output shows that PW connections in up state have been established. This example uses PE 1.

```
<PE1> display vpls connection vsi user_a verbose
VSI Name: user_a                            Signaling: bgp
```

```
  **Remote Vsi ID   : 500
    VC State        : up
    Encapsulation   : ethernet
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 3.3.3.9
    PW Type         : label
    Local VC Label  : 89766
    Remote VC Label : 81922
    Link ID         : 1
    Tunnel Policy   : --
    Tunnel ID       : 0x4600068
VSI Name: user_a                                Signaling: bgp
  **Remote Vsi ID   : 500
    VC State        : up
    Encapsulation   : ethernet
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 4.4.4.9
    PW Type         : label
    Local VC Label  : 89767
    Remote VC Label : 81973
    Link ID         : 1
    Tunnel Policy   : --
    Tunnel ID       : 0x4600069
```

Configuration files

- PE 1:

```
#
 mpls lsr-id 1.1.1.9
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
vsi user_a auto
 pwsignal bgp
  route-distinguisher 100:1
  vpn-target 111:1 import-extcommunity
  vpn-target 111:1 export-extcommunity
  site 1 range 12 default-offset 0
 encapsulation ethernet
#
```

```
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a access-mode ethernet
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_a access-mode ethernet
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
bgp 100
 undo synchronization
 peer 4.4.4.9 as-number 100
 peer 3.3.3.9 as-number 100
 peer 4.4.4.9 connect-interface LoopBack0
 peer 3.3.3.9 connect-interface LoopBack0
 #
 vpls-family
  peer 3.3.3.9 enable
  peer 4.4.4.9 enable
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
```

- PE 2:

```
#
 mpls lsr-id 3.3.3.9
#
mpls
 lsp-trigger all
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
vsi user_a auto
 pwsignal bgp
```

```
  route-distinguisher 100:1
  vpn-target 111:1 import-extcommunity
  vpn-target 111:1 export-extcommunity
  site 2 range 12 default-offset 0
 encapsulation ethernet
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port access vlan 3
#
interface GigabitEthernet2/0/2
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a access-mode ethernet
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_a access-mode ethernet
#
bgp 100
 undo synchronization
 peer 1.1.1.9 as-number 100
 peer 4.4.4.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 peer 4.4.4.9 connect-interface LoopBack0
 #
 vpls-family
  peer 1.1.1.9 enable
  peer 4.4.4.9 enable
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
```

- PE 3:

```
#
 mpls lsr-id 4.4.4.9
#
mpls
 lsp-trigger all
#
l2vpn
```

```
 mpls l2vpn
#
mpls ldp
#
vsi user_a auto
 pwsignal bgp
  route-distinguisher 100:1
  vpn-target 111:1 import-extcommunity
  vpn-target 111:1 export-extcommunity
  site 3 range 12 default-offset 0
 encapsulation ethernet
#
interface LoopBack0
 ip address 4.4.4 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.3.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 port access vlan 4
#
interface GigabitEthernet2/0/2
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a access-mode ethernet
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_a access-mode ethernet
#
bgp 100
 undo synchronization
 peer 1.1.1.9 as-number 100
 peer 3.3.3.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 peer 3.3.3.9 connect-interface LoopBack0
 #
 vpls-family
  peer 1.1.1.9 enable
  peer 3.3.3.9 enable
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 4.4.4.9 0.0.0.0
```

- P:

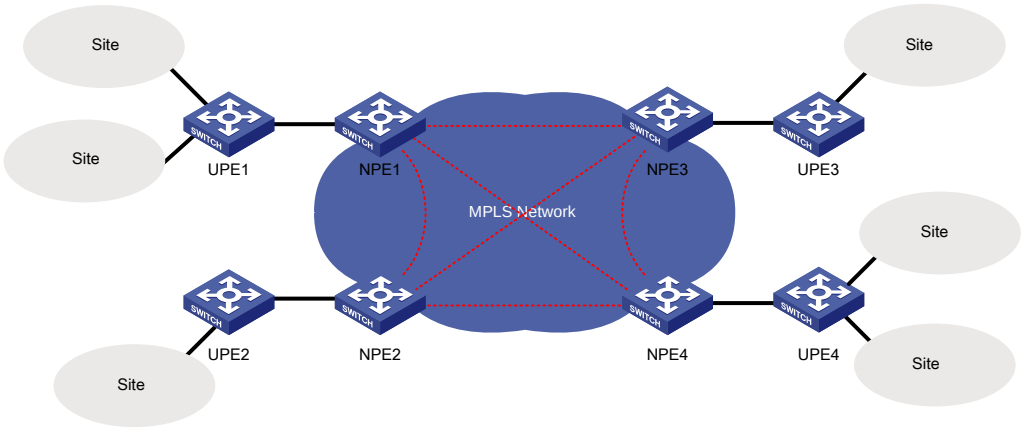
```
#
```

```
 mpls lsr-id 2.2.2.9
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface4
 ip address 10.1.3.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
interface GigabitEthernet2/0/3
 port access vlan 3
#
interface GigabitEthernet2/0/4
 port access vlan 4
#
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
  network 10.1.3.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
```

Example: Configuring H-VPLS with LSP access

H-VPLS classifies PEs into UPEs (user facing provider edge device) and NPEs (network provider edge device). Each UPE connects to the nearest NPE, provides access for user sites, and exchanges packets with remote sites through NPEs that are fully meshed. NPEs must have high performance because they need to process traffic for multiple VPNs.

Figure 244 A basic H-VPLS network



Applicable product matrix

Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 245, a customer's branches are connected to an MPLS backbone through UPEs that support MPLS L2VPN. Configure H-VPLS with LSP access so the branches can communicate with each other at Layer 2.

Figure 245 Network diagram

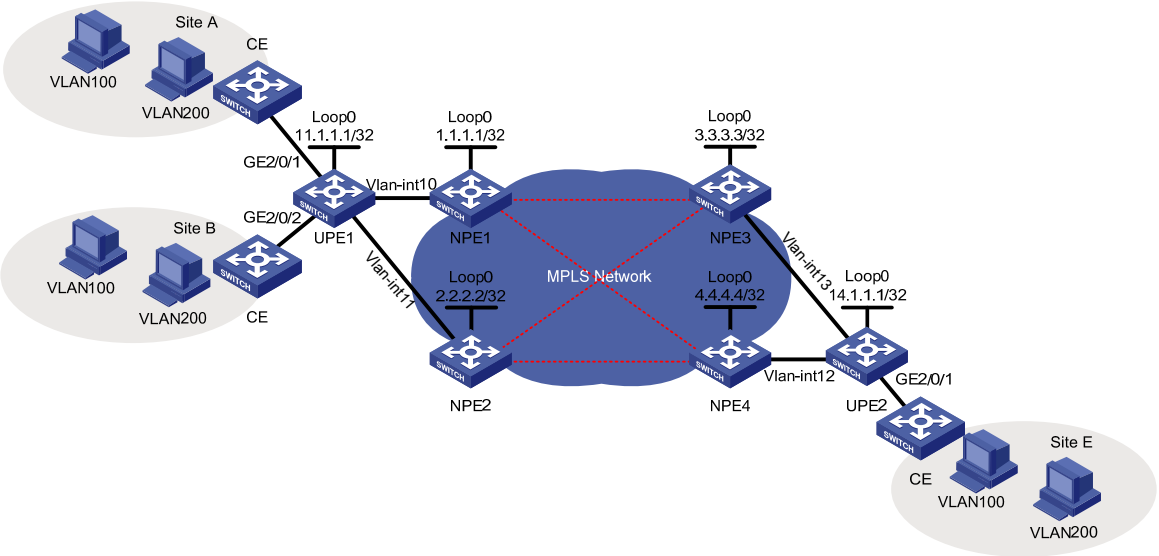


Table 22 Interface and IP assignment

Device	Interface	IP address	Device	Interface	IP address
UPE1	Loop0	11.1.1.1/32	UPE2	Loop0	14.1.1.1/32
	Vlan-int10	11.1.2.1/24		Vlan-int12	20.1.1.1/24
	Vlan-int11	11.1.3.1/24		Vlan-int13	20.1.2.1/24
NPE1	Loop0	1.1.1.1/32	NPE3	Loop0	3.3.3.3/32
	Vlan-int10	11.1.2.2/24		Vlan-int13	20.1.2.2/24
NPE2	Loop0	2.2.2.2/32	NPE4	Loop0	4.4.4.4/32
	Vlan-int11	11.1.3.2/24		Vlan-int12	20.1.1.2/24

Requirements analysis

To negotiate inner labels, perform the following configurations:

- Configure each UPE and all the NPEs connected to the UPE as LDP peers.
- Configure any two NPEs that connects different UPEs as LDP peers.

To achieve NPE redundancy, configure the NPEs that are connected to each UPE as primary and backup peers.

To identify packets to be transported by VPLS, configure service instances and match criteria on the downlink ports of UPEs.

Configuration procedures

Configuring basic settings

1. Create interfaces on UPE and NPE devices and configure IP addresses for the interfaces as shown in Figure 245. (Details not shown.)
2. Configure an IGP protocol on the MPLS backbone to make sure the interfaces of NPE and UPE devices are reachable to each other. (Details not shown.)
3. Configure LDP for label distribution and LSP establishment on NPE and UPE devices. (Details not shown.)
4. Configure the ports of CEs connecting the UPEs as trunk ports that permit packets tagged with VLAN 100 or VLAN 200. (Details not shown.)

Configuring UPE 1

1. Configure basic MPLS.

```
<UPE1> system-view
[UPE1] mpls lsr-id 11.1.1.1
[UPE1] mpls
[UPE1-mpls] quit
[UPE1] mpls ldp
[UPE1-mpls-ldp] quit
```

2. Configure basic MPLS on the interface connecting NPE 1.

```
[UPE1] interface vlan-interface 10
```

```
[UPE1-Vlan-interface10] mpls
[UPE1-Vlan-interface10] mpls ldp
[UPE1-Vlan-interface10] quit
```

3. Configure basic MPLS on the interface connecting NPE 2.

```
[UPE1] interface vlan-interface 11
[UPE1-Vlan-interface11] mpls
[UPE1-Vlan-interface11] mpls ldp
[UPE1-Vlan-interface11] quit
```

4. Establish an LDP session to NPE 1.

```
[UPE1] mpls ldp remote-peer 1
[UPE1-mpls-remote-1] remote-ip 1.1.1.1
[UPE1-mpls-remote-1] quit
```

5. Establish an LDP session to NPE 2.

```
[UPE1] mpls ldp remote-peer 2
[UPE1-mpls-remote-2] remote-ip 2.2.2.2
[UPE1-mpls-remote-2] quit
```

6. Enable MPLS L2VPN.

```
[UPE1] l2vpn
[UPE1-l2vpn] mpls l2vpn
[UPE1-l2vpn] quit
```

7. Create a VPLS instance named **user_a** and use LDP as the signaling protocol. (You can also use BGP as the signaling protocol. See" Example: Configuring full-mesh VPLS using BGP.")

```
[UPE1] vsi user_a static
[UPE1-vsi-user_a] pwsignal ldp
```

8. Set the VSI ID of the VPLS instance to 500. The VSI ID must be unique on the MPLS network.

```
[UPE1-vsi-user_a-ldp] vsi-id 500
```

9. Configure NPE 1 as the primary peer and NPE 2 as the backup peer (use the link to NPE 1 as the primary PW and the link to NPE 2 as the backup PW).

```
[UPE1-vsi-user_a-ldp] peer 1.1.1.1 backup-peer 2.2.2.2
```

10. Configure the reverting wait time as 10 minutes. If the primary PW recovers after a primary/backup failover, the device waits for 10 minutes before it switches traffic back to the primary PW.

```
[UPE1-vsi-user_a-ldp] dual-npe revertive wtr-time 10
[UPE1-vsi-user_a-ldp] quit
[UPE1-vsi-user_a] quit
```

11. On GigabitEthernet 2/0/1 that connects to Site A, create service instance 1000 to match packets from VLAN 100. Bind the service instance with VPLS instance **user_a** so that the matching packets will be transmitted by the VPLS instance.

```
[UPE1] interface gigabitethernet 2/0/1
[UPE1-GigabitEthernet2/0/1] service-instance 1000
[UPE1-GigabitEthernet2/0/1-srv1000] encapsulation s-vid 100
[UPE1-GigabitEthernet2/0/1-srv1000] xconnect vsi user_a
[UPE1-GigabitEthernet2/0/1-srv1000] quit
```

12. On GigabitEthernet 2/0/1, create service instance 2000 to match packets from VLAN 200. Bind the service instance with VPLS instance **user_a** so that the matching packets will be transmitted by the VPLS instance.

```
[UPE1-GigabitEthernet2/0/1] service-instance 2000
```

```
[UPE1-GigabitEthernet2/0/1-srv2000] encapsulation s-vid 200
[UPE1-GigabitEthernet2/0/1-srv2000] xconnect vsi user_a
[UPE1-GigabitEthernet2/0/1-srv2000] quit
```

13. On GigabitEthernet 2/0/2 that connects to Site B, create service instance 1000 and service instance 2000 to match packets from VLAN 100 and VLAN 200, respectively. Bind the service instances with VPLS instance **user_a**.

```
[UPE1] interface gigabitethernet 2/0/2
[UPE1-GigabitEthernet2/0/2] service-instance 1000
[UPE1-GigabitEthernet2/0/2-srv1000] encapsulation s-vid 100
[UPE1-GigabitEthernet2/0/2-srv1000] xconnect vsi user_a
[UPE1-GigabitEthernet2/0/2-srv1000] quit
[UPE1-GigabitEthernet2/0/2] service-instance 2000
[UPE1-GigabitEthernet2/0/2-srv2000] encapsulation s-vid 200
[UPE1-GigabitEthernet2/0/2-srv2000] xconnect vsi user_a
[UPE1-GigabitEthernet2/0/2-srv2000] quit
```

Configuring NPE 1

1. Configure basic MPLS on the interface connecting UPE 1.

```
<NPE1> system-view
[NPE1] interface vlan-interface 10
[NPE1-Vlan-interface10] mpls
[NPE1-Vlan-interface10] mpls ldp
[NPE1-Vlan-interface10] quit
```

2. Establish a remote LDP session to UPE 1.

```
[NPE1] mpls ldp remote-peer 1
[NPE1-mpls-remote-1] remote-ip 11.1.1.1
[NPE1-mpls-remote-1] quit
```

3. Establish a remote LDP session to UPE 3.

```
[NPE1] mpls ldp remote-peer 2
[NPE1-mpls-remote-2] remote-ip 3.3.3.3
[NPE1-mpls-remote-2] quit
```

4. Establish a remote LDP session to UPE 4.

```
[NPE1] mpls ldp remote-peer 3
[NPE1-mpls-remote-3] remote-ip 4.4.4.4
[NPE1-mpls-remote-3] quit
```

5. Configure MPLS L2VPN.

```
[NPE1] l2vpn
[NPE1-l2vpn] mpls l2vpn
[NPE1-l2vpn] quit
```

6. Create VPLS Instance **user_a** and use LDP as the signaling protocol.

```
[NPE1] vsi user_a static
[NPE1-vsi-user_a] pwsignal ldp
```

7. Configure the VSI ID for the VPLS instance. The VSI ID must be consistent with that configured on UPE 1.

```
[NPE1-vsi-user_a-ldp] vsi-id 500
```

8. Configure UPE 1 as the LDP peer of NPE 1.

```
[NPE1-vsi-user_a-ldp] peer 11.1.1.1 upe
```

9. Configure NPE 3 and NPE 4 as the LDP peers of NPE 1.

```
[NPE1-vsi-user_a-ldp] peer 3.3.3.3
[NPE1-vsi-user_a-ldp] peer 4.4.4.4
[NPE1-vsi-user_a-ldp] quit
[NPE1-vsi-user_a] quit
```

Configuring NPE 2

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

Configuring UPE 2

1. Configure basic MPLS.

```
<UPE2> system-view
[UPE2] mpls lsr-id 14.1.1.1
[UPE2] mpls
[UPE2-mpls] quit
[UPE2] mpls ldp
[UPE2-mpls-ldp] quit
```

2. Configure basic MPLS on the interface connecting NPE 3.

```
[UPE2] interface vlan-interface 13
[UPE2-Vlan-interface13] mpls
[UPE2-Vlan-interface13] mpls ldp
[UPE2-Vlan-interface13] quit
```

3. Configure basic MPLS on the interface connecting NPE 4.

```
[UPE2] interface vlan-interface 12
[UPE2-Vlan-interface12] mpls
[UPE2-Vlan-interface12] mpls ldp
[UPE2-Vlan-interface12] quit
```

4. Establish a remote LDP session to NPE 3.

```
[UPE2] mpls ldp remote-peer 1
[UPE2-mpls-remote-1] remote-ip 3.3.3.3
[UPE2-mpls-remote-1] quit
```

5. Establish a remote LDP session to NPE 4.

```
[UPE2] mpls ldp remote-peer 2
[UPE2-mpls-remote-2] remote-ip 4.4.4.4
[UPE2-mpls-remote-2] quit
```

6. Enable MPLS L2VPN.

```
[UPE2] l2vpn
[UPE2-l2vpn] mpls l2vpn
[UPE2-l2vpn] quit
```

7. Create a VPLS instance named **user_a** and use LDP as the signaling protocol.

```
[UPE2] vsi user_a static
[UPE2-vsi-user_a] pwsignal ldp
```

8. Set the VSI ID of the VPLS instance to 500. The VSI ID must be the same as that configured on UPE 1.

```
[UPE2-vsi-user_a-ldp] vsi-id 500
```

9. Configure NPE 3 as the peer and NPE 4 as the backup peer (use the link to NPE 3 as the primary PW and use the link to NPE 4 as the backup PW).

```
[UPE2-vsi-user_a-ldp] peer 3.3.3.3 backup-peer 4.4.4.4
```

10. Configure the reverting wait time as 10 minutes. If the primary PW recovers after a primary/backup failover, the device waits for 10 minutes before it switches traffic back to the primary PW.

```
[UPE2-vsi-user_a-ldp] dual-npe revertive wtr-time 10
[UPE2-vsi-user_a-ldp] quit
[UPE2-vsi-user_a] quit
```

11. On GigabitEthernet 2/0/1 (the interface connected to Site E), create service instance 1000, match VLAN 100, and bind the service instance to VPLS instance **user_a**.

```
[UPE2] interface gigabitethernet 2/0/1
[UPE2-GigabitEthernet2/0/1] service-instance 1000
[UPE2-GigabitEthernet2/0/1-srv1000] encapsulation s-vid 100
[UPE2-GigabitEthernet2/0/1-srv1000] xconnect vsi user_a
[UPE2-GigabitEthernet2/0/1-srv1000] quit
```

12. Create service instance 2000, match VLAN 200, and bind the service instance to VPLS instance **user_a**.

```
[UPE2-GigabitEthernet2/0/1] service-instance 2000
[UPE2-GigabitEthernet2/0/1-srv2000] encapsulation s-vid 200
[UPE2-GigabitEthernet2/0/1-srv2000] xconnect vsi user_a
[UPE2-GigabitEthernet2/0/1-srv2000] quit
```

Configuring NPE 3

1. Configure basic MPLS on the interface connecting UPE 2.

```
[NPE3] interface vlan-interface 13
[NPE3-Vlan-interface13] mpls
[NPE3-Vlan-interface13] mpls ldp
[NPE3-Vlan-interface13] quit
```

2. Establish a remote LDP session to UPE 2.

```
[NPE3] mpls ldp remote-peer 1
[NPE3-mpls-remote-1] remote-ip 14.1.1.1
[NPE3-mpls-remote-1] quit
```

3. Establish a remote LDP session to NPE 1.

```
[NPE3] mpls ldp remote-peer 2
[NPE3-mpls-remote-2] remote-ip 1.1.1.1
[NPE3-mpls-remote-2] quit
```

4. Establish a remote LDP session to NPE 2.

```
[NPE3] mpls ldp remote-peer 3
[NPE3-mpls-remote-3] remote-ip 2.2.2.2
[NPE3-mpls-remote-3] quit
```

5. Configure MPLS L2VPN.

```
[NPE3] l2vpn
[NPE3-l2vpn] mpls l2vpn
[NPE3-l2vpn] quit
```

6. Create VPLS Instance **user_a** and use LDP as the signaling protocol.

```
[NPE3] vsi user_a static
[NPE3-vsi-user_a] pwsignal ldp
```

7. Configure the VSI ID for the VPLS instance as 500. The VSI ID must be consistent with that configured on UPE 1.

```
[NPE3-vsi-user_a-ldp] vsi-id 500
```

8. Configure UPE 2 as the LDP peer of NPE 3.

```
[NPE3-vsi-user_a-ldp] peer 14.1.1.1 upe
```

9. Configure NPE 1 and NPE 2 as the LDP peers of NPE 3.

```
[NPE3-vsi-user_a-ldp] peer 1.1.1.1
[NPE3-vsi-user_a-ldp] peer 2.2.2.2
[NPE3-vsi-user_a-ldp] quit
[NPE3-vsi-user_a] quit
```

Configuring NPE 4

Configure NPE 4 in the same way that NPE 3 is configured. (Details not shown.)

Verifying the configuration

On each UPE and NPE, display the PW status. This example uses UPE 1 and NPE 1:

On UPE 1, execute the **display vpls connection** command to view the PW status.

```
<UPE1> display vpls connection vsi user_a
Total 2 connection(s),
connection(s): 1 up, 1 block, 0 down, 2 ldp, 0 bgp

VSI Name: user_a                          Signaling: ldp
VsiID   VsiType   PeerAddr   InLabel   OutLabel   LinkID   VCState
500     vlan      1.1.1.1    1024      1025       1        up
500     vlan      2.2.2.2    1026      1027       2        block
```

On NPE 1, execute the **display vpls connection** command to view the PW status.

```
<NPE1> display vpls connection vsi user_a
Total 3 connection(s),
connection(s): 3 up, 0 block, 0 down, 3 ldp, 0 bgp

VSI Name: user_a                          Signaling: ldp
VsiID   VsiType   PeerAddr   InLabel   OutLabel   LinkID   VCState
500     vlan      3.3.3.3    1030      1031       1        up
500     vlan      4.4.4.4    1028      1029       2        up
500     vlan      11.1.1.1   1025      1024       3        up
```

Use the **ping** command to check the connectivity between hosts at different sites. If they can ping each other, you can conclude that the L2VPN has been established.

Configuration files

The following lists only the H-VPLS-related configuration files. CE configuration and PE routing protocol configurations are not shown.

- UPE 1:

```
#
 mpls lsr-id 11.1.1.1
```

```
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 1.1.1.1
#
mpls ldp remote-peer 2
 remote-ip 2.2.2.2
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 1.1.1.1 backup-peer 2.2.2.2
  dual-npe revertive wtr-time 10
#
interface LoopBack0
 ip address 11.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 11.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface11
 ip address 11.1.3.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 2000
  encapsulation s-vid 200
  xconnect vsi user_a
#
interface GigabitEthernet2/0/2
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 2000
  encapsulation s-vid 200
  xconnect vsi user_a
```

- NPE 1:

```
#
 mpls lsr-id 1.1.1.1
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 11.1.1.1
#
mpls ldp remote-peer 2
 remote-ip 3.3.3.3
#
mpls ldp remote-peer 3
 remote-ip 4.4.4.4
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 11.1.1.1 upe
  peer 3.3.3.3
  peer 4.4.4.4
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 11.1.2.2 255.255.255.0
 mpls
 mpls ldp
```

- NPE 2:

```
#
 mpls lsr-id 2.2.2.2
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 11.1.1.1
#
```

```
mpls ldp remote-peer 2
 remote-ip 3.3.3.3
#
mpls ldp remote-peer 3
 remote-ip 4.4.4.4
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 11.1.1.1 upe
  peer 3.3.3.3
  peer 4.4.4.4
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface10
 ip address 11.1.3.2 255.255.255.0
 mpls
 mpls ldp
```

- UPE 2:

```
#
 mpls lsr-id 14.1.1.1
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.3
#
mpls ldp remote-peer 2
 remote-ip 4.4.4.4
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 3.3.3.3 backup-peer 4.4.4.4
  dual-npe revertive wtr-time 10
#
interface LoopBack0
 ip address 14.1.1.1 255.255.255.255
#
interface Vlan-interface12
 ip address 20.1.1.1 255.255.255.0
```

```
 mpls
 mpls ldp
#
interface Vlan-interface13
 ip address 20.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/1
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 2000
  encapsulation s-vid 200
  xconnect vsi user_a
```

- NPE 3:

```
#
 mpls lsr-id 3.3.3.3
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 14.1.1.1
#
mpls ldp remote-peer 2
 remote-ip 1.1.1.1
#
mpls ldp remote-peer 3
 remote-ip 2.2.2.2
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 14.1.1.1 upe
  peer 1.1.1.1
  peer 2.2.2.2
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface13
 ip address 20.1.2.2 255.255.255.0
 mpls
```

```
 mpls ldp
```

- NPE 4:

```
#
 mpls lsr-id 4.4.4.4
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 14.1.1.1
#
mpls ldp remote-peer 2
 remote-ip 1.1.1.1
#
mpls ldp remote-peer 3
 remote-ip 2.2.2.2
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 14.1.1.1 upe
  peer 1.1.1.1
  peer 2.2.2.2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface12
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls ldp
```

Example: Configuring H-VPLS with QinQ access

Applicable product matrix

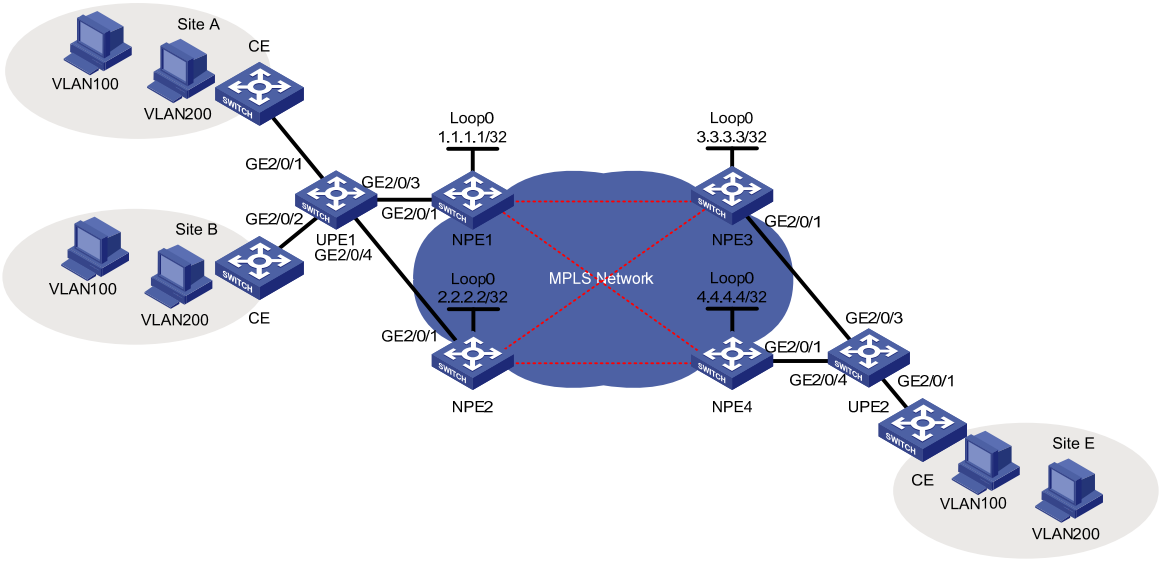
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 246, a customer's branches are connected to an MPLS backbone through UPEs that do not support MPLS L2VPN.

Configure H-VPLS with QinQ access so the branches can communicate with each other at Layer 2.

Figure 246 Network diagram



Requirements analysis

For NPEs to identify user traffic, enable QinQ and add an outer tag (the provider VLAN tag) to upstream packets on the downlink port of each UPE.

If a UPE is connected to two NPEs, use STP to prevent loops and implement link redundancy.

To forward packets from an UPE through the bound PW, configure service instances to match the outer provider tag of packets on the downlink port of each NPE.

To negotiate inner labels, configure any two NPEs that connect to different UPEs as LDP peers.

Configuration procedures

Configuring basic settings

1. Configure an IGP on the MPLS backbone to make sure the interfaces of NPE devices are reachable to each other. (Details not shown.)
2. Configure LDP for label distribution and LSP establishment on the MPLS backbone. (Details not shown.)
3. Configure the ports of CEs connecting the UPEs as trunk ports that permit packets tagged with VLAN 100 or VLAN 200. (Details not shown.)

Configuring UPE 1

1. On GigabitEthernet 2/0/1, enable QinQ, and add an outer provider VLAN tag of 1000 to packets.

```
<UPE1> system-view
[UPE1] interface GigabitEthernet 2/0/1
[UPE1-GigabitEthernet2/0/1] port access vlan 1000
[UPE1-GigabitEthernet2/0/1] qinq enable
[UPE1-GigabitEthernet2/0/1] quit
```

2. On GigabitEthernet 2/0/2, enable QinQ, and add an outer provider VLAN tag of 1000 to packets.

```
[UPE1] interface GigabitEthernet 2/0/2
[UPE1-GigabitEthernet2/0/2] port access vlan 1000
[UPE1-GigabitEthernet2/0/2] qinq enable
[UPE1-GigabitEthernet2/0/2] quit
```

3. Configure GigabitEthernet 2/0/3 as a trunk port that allows forwarding packets tagged with VLAN 1000 to NPE 1.

```
[UPE1] interface GigabitEthernet 2/0/3
[UPE1-GigabitEthernet2/0/3] port link-type trunk
[UPE1-GigabitEthernet2/0/3] port trunk permit vlan 1000
[UPE1-GigabitEthernet2/0/3] quit
```

4. Configure GigabitEthernet 2/0/4 as a trunk port that allows forwarding packets tagged with VLAN 1000 to NPE 2.

```
[UPE1] interface GigabitEthernet 2/0/4
[UPE1-GigabitEthernet2/0/4] port link-type trunk
[UPE1-GigabitEthernet2/0/4] port trunk permit vlan 1000
[UPE1-GigabitEthernet2/0/4] quit
```

Configuring NPE1

Establish a remote LDP session to NPE 3.

```
[NPE1] mpls ldp remote-peer 1
[NPE1-mpls-ldp-remote-1] remote-ip 3.3.3.3
[NPE1-mpls-ldp-remote-1] quit
```

Establish a remote LDP session to NPE 4.

```
[NPE1] mpls ldp remote-peer 2
[NPE1-mpls-ldp-remote-2] remote-ip 4.4.4.4
[NPE1-mpls-ldp-remote-2] quit
```

Create VLAN instance **user_a**. Because the upstream packets carry the provider VLAN tag and need to be transmitted to the peer NPE, you must configure the encapsulation type for the VPLS instance as **VLAN**. (The default encapsulation type is VLAN.)

```
[NPE1] vsi user_a static
[NPE1-vsi-user_a] encapsulation vlan
```

Configure the signaling protocol as LDP.

```
[NPE1-vsi-user_a] pwsignal ldp
```

Set the VSI ID of the VPLS instance to 500. The VSI ID must be unique on the MPLS network.

```
[NPE1-vsi-user_a-ldp] vsi-id 500
```

Configure NPE 3 and NPE 4 as the remote LDP peers of NPE 1.

```
[NPE1-vsi-user_a-ldp] peer 3.3.3.3
[NPE1-vsi-user_a-ldp] peer 4.4.4.4
[NPE1-vsi-user_a-ldp] quit
```

```
[NPE1-vsi-user_a] quit
```

On GigabitEthernet 2/0/1 that connects UPE 1, create service instance 1000 to match packets from VLAN 100. Bind the service instance with VPLS instance **user_a**. Because the upstream packets carry the provider VLAN, you must configure the AC access mode as **VLAN**. (The default access mode is VLAN.)

```
[NPE1] interface gigabitethernet 2/0/1
[NPE1-GigabitEthernet2/0/1] service-instance 1000
[NPE1-GigabitEthernet2/0/1-srv1000] encapsulation s-vid 1000
[NPE1-GigabitEthernet2/0/1-srv1000] xconnect vsi user_a access-mode vlan
[NPE1-GigabitEthernet2/0/1-srv1000] quit
```

Configuring NPE 2

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

Configuring UPE 2

1. On GigabitEthernet 2/0/1, enable QinQ, and add an outer provider VLAN tag of 1000 to packets. The VLAN tag must be the same as that configured on UPE 1.

   ```
   <UPE2> system-view
   [UPE2] interface GigabitEthernet 2/0/1
   [UPE2-GigabitEthernet2/0/1] port access vlan 1000
   [UPE2-GigabitEthernet2/0/1] qinq enable
   [UPE2-GigabitEthernet2/0/1] quit
   ```

2. Configure GigabitEthernet 2/0/3 as a trunk port that allows forwarding packets tagged with VLAN 1000 to NPE 3.

   ```
   [UPE2] interface GigabitEthernet 2/0/3
   [UPE2-GigabitEthernet2/0/3] port link-type trunk
   [UPE2-GigabitEthernet2/0/3] port trunk permit vlan 1000
   [UPE2-GigabitEthernet2/0/3] quit
   ```

3. Configure GigabitEthernet 2/0/4 as a trunk port that allows forwarding packets tagged with VLAN 1000 to NPE 4.

   ```
   [UPE2] interface GigabitEthernet 2/0/4
   [UPE2-GigabitEthernet2/0/4] port link-type trunk
   [UPE2-GigabitEthernet2/0/4] port trunk permit vlan 1000
   [UPE2-GigabitEthernet2/0/4] quit
   ```

Configuring NPE 3

Establish a remote LDP session to NPE 1.

```
<NPE3> system-view
[NPE3] mpls ldp remote-peer 1
[NPE3-mpls-remote-1] remote-ip 1.1.1.1
[NPE3-mpls-remote-1] quit
```

Establish a remote LDP session to NPE 2.

```
[NPE3] mpls ldp remote-peer 2
[NPE3-mpls-remote-2] remote-ip 2.2.2.2
[NPE3-mpls-remote-2] quit
```

Enable MPLS L2VPN.

```
[NPE3] l2vpn
[NPE3-l2vpn] mpls l2vpn
[NPE3-l2vpn] quit
```

Create VPLS instance **user_a**. Because the upstream packets carry the provider VLAN tag and need to be transmitted to the peer NPE, you must configure the encapsulation type for the VPLS instance as **VLAN**. (The default encapsulation type is VLAN.)

```
[NPE3] vsi user_a static
[NPE3-vsi-user_a] encapsulation vlan
```

Configure the signaling protocol as LDP.

```
[NPE3-vsi-user_a] pwsignal ldp
```

Configure the VSI ID for the VPLS instance. The VSI ID must be consistent with that configured on NPE 1.

```
[NPE3-vsi-user_a-ldp] vsi-id 500
```

Configure NPE 1 and NPE 2 as the LDP peers of NPE 3.

```
[NPE3-vsi-user_a-ldp] peer 1.1.1.1
[NPE3-vsi-user_a-ldp] peer 2.2.2.2
[NPE3-vsi-user_a-ldp] quit
[NPE3-vsi-user_a] quit
```

On GigabitEthernet 2/0/1 that connects UPE 2, create service instance 1000 to match packets from VLAN 100 and bind the service instance with VPLS instance **user_a**. Because the upstream packets carry the provider VLAN, you must configure the AC access mode as VLAN. (The default access mode is VLAN.)

```
[NPE3] interface gigabitethernet 2/0/1
[NPE3-GigabitEthernet2/0/1] service-instance 1000
[NPE3-GigabitEthernet2/0/1-srv1000] encapsulation s-vid 1000
[NPE3-GigabitEthernet2/0/1-srv1000] xconnect vsi user_a access-mode vlan
[NPE3-GigabitEthernet2/0/1-srv1000] quit
```

Configuring NPE 4

Configure NPE 4 in the same way that NPE 3 is configured. (Details not shown.)

Configuring loop prevention

You do not need to configure MSTP because MSTP is enabled by default.

Verifying the configuration

On each NPE, display the PW status by using the **display vpls connection** command. This example uses NPE 1.

```
<NPE1> display vpls connection vsi user_a
Total 2 connection(s),
connection(s): 2 up, 0 block, 0 down, 2 ldp, 0 bgp

VSI Name: user_a                          Signaling: ldp
VsiID   VsiType   PeerAddr   InLabel   OutLabel   LinkID   VCState
500     vlan      3.3.3.3    1030      1031       1        up
500     vlan      4.4.4.4    1028      1029       2        up
```

Use the **ping** command to check the connectivity between hosts at different sites. If they can ping each other, you can conclude that the L2VPN has been established.

Configuration files

The following lists only the H-VPLS-related configuration files. CE configuration and PE routing protocol configurations are not shown.

- UPE 1:

```
#
interface GigabitEthernet2/0/1
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet2/0/2
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet2/0/3
 port link-type trunk
 port trunk permit vlan 1 1000
#
interface GigabitEthernet2/0/4
 port link-type trunk
 port trunk permit vlan 1 1000
```

- NPE 1:

```
#
 mpls lsr-id 1.1.1.1
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.3
#
mpls ldp remote-peer 2
 remote-ip 4.4.4.4
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 3.3.3.3
  peer 4.4.4.4
#
interface GigabitEthernet2/0/1
 service-instance 1000
  encapsulation s-vid 1000
```

```
  xconnect vsi user_a
```

- NPE 2:

```
#
 mpls lsr-id 2.2.2.2
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 3.3.3.3
#
mpls ldp remote-peer 2
 remote-ip 4.4.4.4
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 3.3.3.3
  peer 4.4.4.4
#
interface GigabitEthernet2/0/1
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
```

- UPE 2:

```
#
interface GigabitEthernet2/0/1
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet2/0/3
 port link-type trunk
 port trunk permit vlan 1 1000
#
interface GigabitEthernet2/0/4
 port link-type trunk
 port trunk permit vlan 1 1000
```

- NPE 3:

```
#
 mpls lsr-id 3.3.3.3
#
mpls
#
l2vpn
```

```
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 1.1.1.1
#
mpls ldp remote-peer 2
 remote-ip 2.2.2.2
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 1.1.1.1
  peer 2.2.2.2
#
interface GigabitEthernet2/0/1
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
```

- NPE 4:

```
#
 mpls lsr-id 4.4.4.4
#
mpls
#
l2vpn
 mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 1
 remote-ip 1.1.1.1
#
mpls ldp remote-peer 2
 remote-ip 2.2.2.2
#
vsi user_a static
 pwsignal ldp
  vsi-id 500
  peer 1.1.1.1
  peer 2.2.2.2
#
interface GigabitEthernet2/0/1
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
```

IPv4-based VRRP configuration examples

This chapter provides IPv4-based VRRP configuration examples.

Example: Configuring a single VRRP group

Applicable product matrix

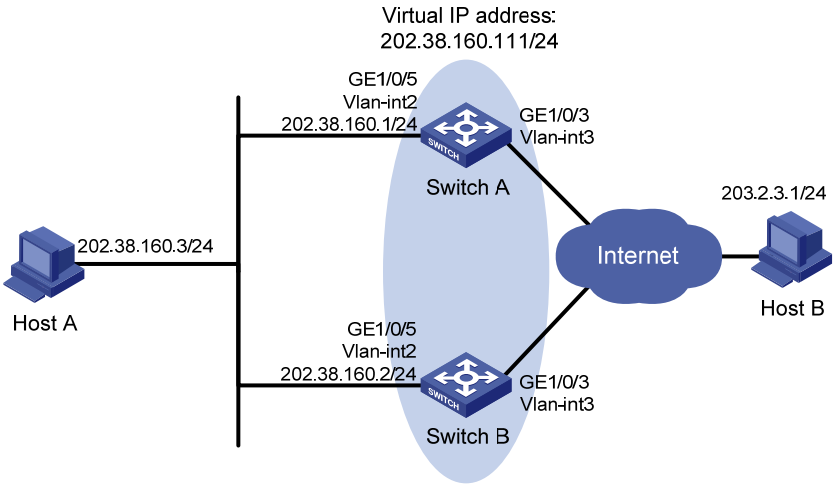
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 247, configure a VRRP group on Switch A and Switch B as the gateway for the hosts, and implement the following requirements:

- Switch A operates as the master to forward packets from the hosts to the external network. When Switch A fails, Switch B takes over to forward packets for the hosts.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 247 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid frequent role change in the VRRP group, configure a preemption delay.

Configure VRRP tracking on Switch A so that when its uplink is not available, Switch A decreases its priority for Switch B to take over quickly.

For switches in the VRRP group to only process authorized packets, configure VRRP authentication.

Configuration restrictions and guidelines

When you configure a sing IPv4 VRRP group, follow these restrictions and guidelines:

- Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to them is also the same.
- When you configure VRRP tracking for a member switch, make sure the reduced priority for the switch is high enough for any other member switch to take over.

Configuration procedures

1. Configure Switch A:

   # Configure VLAN 3.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 3
   [SwitchA-vlan3] port gigabitethernet 1/0/3
   [SwitchA-vlan3] quit
   [SwitchA] interface Vlan-interface 3
   [SwitchA-Vlan-interface3] ip address 100.0.0.2 24
   [SwitchA-Vlan-interface3] quit
   ```

   # Configure VLAN 2.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface Vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
   ```

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 202.38.160.111/24.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
   ```

   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   ```

   # Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
   ```

   # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
   ```

   # Configure VRRP to monitor VLAN-interface 3 on Switch A. When the interface fails, the weight of Switch A decreases by 20 so Switch B can take over.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 3 reduced 20
   ```

2. Configure Switch B:

   # Configure VLAN 3.

   ```
   <SwitchA> system-view
   ```

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] quit
[SwitchB] interface Vlan-interface 3
[SwitchB-Vlan-interface3] ip address 101.0.0.2 24
[SwitchB-Vlan-interface3] quit
```

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-Vlan2] port gigabitethernet 1/0/5
[SwitchB-Vlan2] quit
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 202.38.160.111/24.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

3. Configure Host A.

   Configure the default gateway of Host A as 202.38.160.111. (Details not shown.)

Verifying the configuration

Ping Host B from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 1
     Admin Status   : Up                State         : Master
     Config Pri     : 110               Running Pri   : 110
     Preempt Mode   : Yes               Delay Time    : 5
     Auth Type      : Simple            Key           : ******
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
   VRRP Track Information:
     Track Interface: Vlan3             State : Up        Pri Reduced : 20
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
```

```
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 1
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple             Key          : ******
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.1
```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 1
     Admin Status   : Up                 State        : Master
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 5
     Auth Type      : Simple             Key          : ******
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.2
```

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 1
     Admin Status   : Up                 State        : Backup
     Config Pri     : 110                Running Pri  : 90
     Preempt Mode   : Yes                Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple             Key          : ******
     Virtual IP     : 202.38.160.111
```

```
    Master IP      : 202.38.160.2
  VRRP Track Information:
    Track Interface: Vlan3                State : Down       Pri Reduced : 20
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 1
     Admin Status   : Up                 State         : Master
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : Simple             Key           : ******
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.2
```

The output shows that when VLAN-interface 3 on Switch A fails, the priority of Switch A decreases by 20. Switch A becomes the backup, and Switch B becomes the master to forward packets from Host A to Host B.

Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 202.38.160.1 255.255.255.0
 vrrp vrid 1 virtual-ip 202.38.160.111
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track interface vlan-interface3 reduced 20
 vrrp vrid 1 authentication-mode simple cipher $c$3$1FcANPYJCkyfZyS7FAl0oW8bBcUX
Nbbc
#
interface Vlan-interface3
 ip address 100.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

- Switch B:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 202.38.160.2 255.255.255.0
 vrrp vrid 1 virtual-ip 202.38.160.111
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher $c$3$vxKRiU4Fy/p4dRTiw+znGTQyYNDfQrxb
#
interface Vlan-interface3
 ip address 101.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring VRRP-Track-NQA collaboration for the master to monitor the uplinks

Applicable product matrix

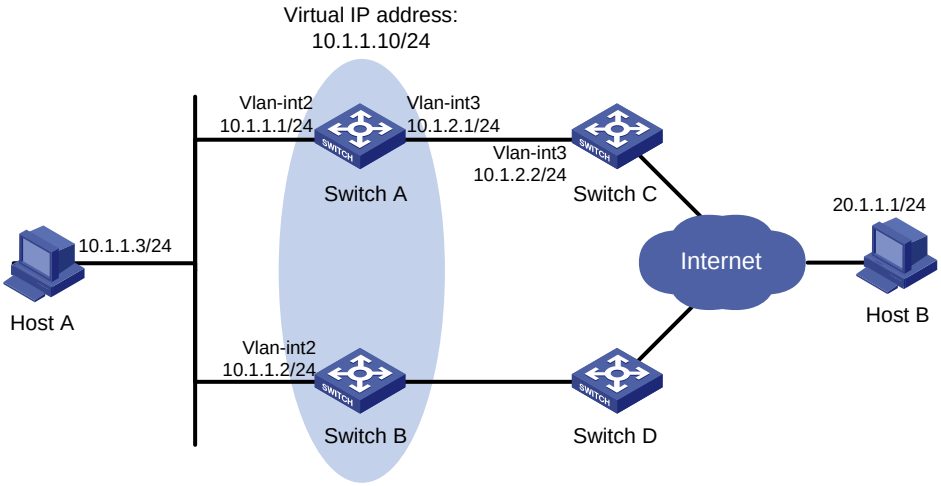
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 248, configure a VRRP group on Switch A and Switch B as the gateway for the hosts, and implement the following requirements:

- Switch A operates as the master to forward packets from the hosts to the external network. When Switch A fails, Switch B takes over to forward packets for the hosts.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 248 Network diagram



Requirements analysis

- For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.
- Configure NQA to monitor the uplink of Switch A so that Switch A decreases its priority for Switch B to take over when its uplink interface fails.
- To avoid frequent role change in the VRRP group, configure a preemption delay.
- For switches in the VRRP group to only process authorized packets, configure VRRP authentication.

Configuration restrictions and guidelines

Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to them is also the same.

Configuration procedures

1. Configure the IP address for each interface based on Figure 248.

   This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way. (Details not shown.)

   # Specify an IP address for VLAN-interface 2 on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface Vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
   [SwitchA-Vlan-interface2] quit
   ```

2. Create an NQA operation on Switch A:

   # Create an NQA operation with administrator name **admin** and operation tag **test**.

   ```
   [SwitchA] nqa entry admin test
   ```

Specify the type of the NQA operation as **icmp-echo**.

```
[SwitchA-nqa-admin-test] type icmp-echo
```

Configure the destination IP address of the ICMP echo operation as 10.1.2.2.

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

Configure the ICMP echo operation to repeat at an interval of 100 milliseconds.

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

Create reaction entry 1. If the number of consecutive probe failures reaches 5, collaboration is triggered.

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

Configure the scheduling parameters for the operation with the administrator name **admin** and operation tag **test**. The test starts now and lasts forever.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

3. Configure a track entry on Switch A:

Create track entry 1, and associate it with reaction entry 1 of the NQA operation.

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

4. Configure VRRP on Switch A:

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.10.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the priority of the router in the VRRP group by 20 when the state of track entry 1 changes to negative.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 20
```

5. Configure VRRP on Switch B:

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
```

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.10.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

6. Configure Host A:

Configure the default gateway of Host A as 10.1.1.10. (Details not shown.)

Verifying the configuration

Ping Host B from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 1
     Admin Status   : Up                 State         : Master
     Config Pri     : 110                Running Pri   : 110
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : Simple             Key           : ******
     Virtual IP     : 10.1.1.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 20
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 1
     Admin Status   : Up                 State         : Backup
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Become Master  : 2200ms left
     Auth Type      : Simple             Key           : ******
     Virtual IP     : 10.1.1.10
     Master IP      : 10.1.1.1
```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

Verify that Host A can still ping Host B. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 1
```

```
    Admin Status   : Up                 State         : Backup
    Config Pri     : 110                Running Pri   : 90
    Preempt Mode   : Yes                Delay Time    : 5
    Become Master  : 2200ms left
    Auth Type      : Simple             Key           : ******
    Virtual IP     : 10.1.1.10
    Master IP      : 10.1.1.2
  VRRP Track Information:
    Track Object   : 1                  State : Negative   Pri Reduced : 20
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 1
     Admin Status   : Up                 State         : Master
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : Simple             Key           : ******
     Virtual IP     : 10.1.1.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.2
```

The output shows that when Switch A fails, the priority of Switch A decreases by 20. Switch A becomes the backup, and Switch B becomes the master to forward packets from Host A to Host B.

Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track 1 reduced 20
 vrrp vrid 1 authentication-mode simple cipher $c$3$Fq7Gw6ux6gf6sjUnaPxfYaJSJ08r
xGhc
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
#
```

```
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
nqa entry admin test
 type icmp-echo
  destination ip 10.1.2.2
  frequency 100
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
 track 1 nqa entry admin test reaction 1
#
 nqa schedule admin test start-time now lifetime forever
#
```

- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.10
vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher $c$3$1SjZTNgoayfie8IplIGd+p1lI64Q
oDs4
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring VRRP-Track-BFD collaboration for the master to monitor the uplinks

Applicable product matrix

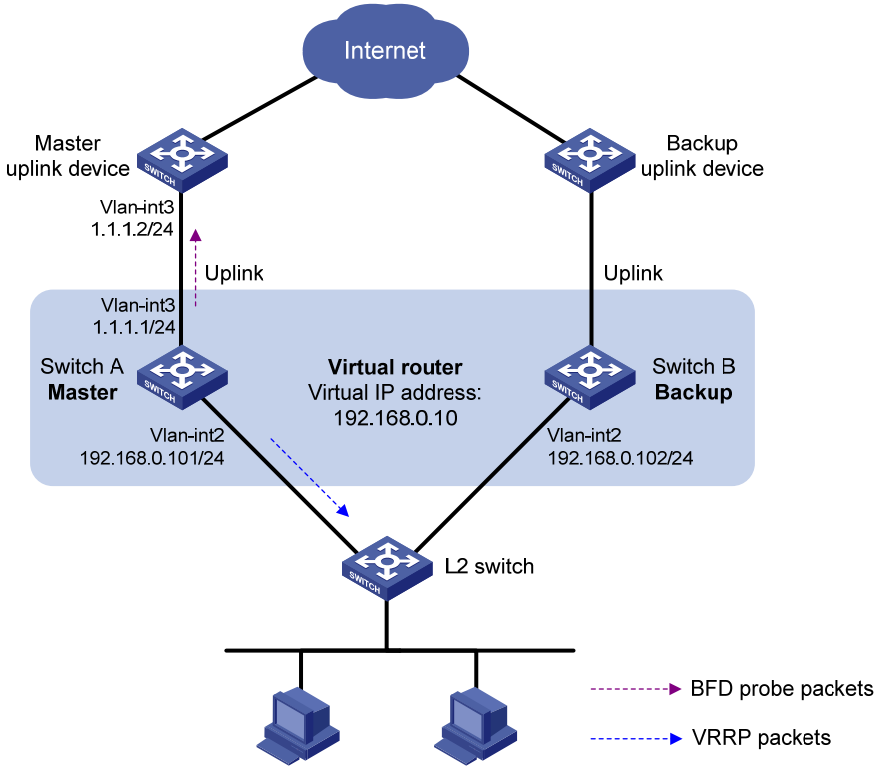
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 249, configure a VRRP group on Switch A and Switch B as the gateway for the hosts, and implement the following requirements:

- Switch A operates as the master to forward packets from the hosts to the external network. When Switch A fails, Switch B takes over to forward packets for the hosts.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 249 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid frequent role change in the VRRP group, configure a preemption delay.

For Switch B to take over quickly when the uplink interface of Switch A fails, configure BFD to monitor the uplink of Switch A. Switch A will decrease its priority when its uplink interface fails.

For switches in the VRRP group to only process authorized packets, configure VRRP authentication.

Configuration restrictions and guidelines

When you configure VRRP-Track-BFD collaboration, follow these restrictions and guidelines:

- Make sure the uplink device of the master supports BFD.

- Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to the switches is also the same.
- Do not configure the local IP address and remote IP address for BFD packets as the virtual IP address of the VRRP group when you configure Track and BFD collaboration.

Configuration procedures

1. Configure the IP address of each VLAN interface as shown in Figure 249. (Details not shown.)

   This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way. (Details not shown.)

   # Specify an IP address for VLAN-interface 2 on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface Vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.0.101 255.255.255.0
   [SwitchA-Vlan-interface2] quit
   ```

2. Configure BFD on Switch A:

   # Specify the source IP address for BFD echo packets as **10.10.10.10**.

   ```
   [SwitchA] bfd echo-source-ip 10.10.10.10
   ```

3. Configure a track entry on Switch A. This track entry uses BFD echo packets to monitor the link between local IP address 1.1.1.1 and remote IP address 1.1.1.2.

   ```
   [SwitchA] track 1 bfd echo interface vlan-interface 3 remote ip 1.1.1.2 local ip
   1.1.1.1
   ```

4. Configure VRRP on Switch A:

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
   ```

   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   ```

   # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
   ```

   # Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
   ```

   # Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the priority of Switch A in the VRRP group by 20 when the state of track entry 1 changes to negative.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 20
   [SwitchA-Vlan-interface2] return
   ```

5. Configure VRRP on Switch B:

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 192.168.0.10.

   ```
   <SwitchB> system-view
   [SwitchB] interface vlan-interface 2
   ```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
[SwitchB-Vlan-interface2] return
```

6. Configure Host A:

   Configure the default gateway of Host A as 192.168.0.10. (Details not shown.)

Verifying the configuration

Display detailed information about VRRP group 1 on Switch A.

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 1
     Admin Status   : Up                State         : Master
     Config Pri     : 110               Running Pri   : 110
     Preempt Mode   : Yes               Delay Time    : 5
     Auth Type      : Simple            Key           : ******
     Virtual IP     : 192.168.0.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.101
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 20
```

Display detailed information about track entry 1 on Switch A.

```
<SwitchA> display track 1
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 1.1.1.2
    Local IP   : 1.1.1.1
```

Display detailed information about VRRP group 1 on Switch B.

```
<SwitchB> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
```

```
  Interface Vlan-interface2
    VRID           : 1                   Adver Timer  : 1
    Admin Status   : Up                  State        : Backup
    Config Pri     : 100                 Running Pri  : 100
    Preempt Mode   : Yes                 Delay Time   : 5
    Become Master  : 2200ms left
    Auth Type      : Simple              Key          : ******
    Virtual IP     : 192.168.0.10
    Master IP      : 192.168.0.101
```

The output shows that when the status of track entry 1 becomes **Positive**, Switch A is the master, and Switch B is the backup.

When the uplink of Switch A goes down, the status of track entry 1 becomes **Negative**.

```
<SwitchA> display track 1
Track ID: 1
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 20 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 1.1.1.2
    Local IP   : 1.1.1.1
```

Display detailed information about VRRP group 1 on Switch A.

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 1
     Admin Status   : Up                  State        : Backup
     Config Pri     : 110                 Running Pri  : 90
     Preempt Mode   : Yes                 Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple              Key          : ******
     Virtual IP     : 192.168.0.10
     Master IP      : 192.168.0.102
   VRRP Track Information:
     Track Object   : 1                   State : Negative   Pri Reduced : 20
```

Display detailed information about VRRP group 1 on Switch B.

```
<SwitchB> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
```

```
VRID            : 1                   Adver Timer   : 1
Admin Status    : Up                  State         : Master
Config Pri      : 100                 Running Pri   : 100
Preempt Mode    : Yes                 Delay Time    : 5
Become Master   : 2200ms left
Auth Type       : Simple              Key           : ******
Virtual IP      : 192.168.0.10
Virtual MAC     : 0000-5e00-0101
Master IP       : 192.168.0.102
```

The output shows that when Switch A detects that the uplink fails through BFD, it decreases its priority to 90 to make sure Switch B can become the master.

Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```
#
 bfd echo-source-ip 10.10.10.10
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.0.101 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 priority 110
vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track 1 reduced 20
 vrrp vrid 1 authentication-mode simple cipher $c$3$8j5zt3i82EKmOjERTrq8BiL906Sv
iDVp
#
interface Vlan-interface3
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
track 1 bfd echo interface Vlan-interface3 remote ip 1.1.1.2 local ip 1.1.1.1
#
```

- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
```

```
 ip address 192.168.0.102 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.10
vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher $c$3$1SjZTNgoayfie8IplIGd+p1lI64Q
oDs4
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring VRRP-Track-BFD collaboration for a backup to monitor the master

Applicable product matrix

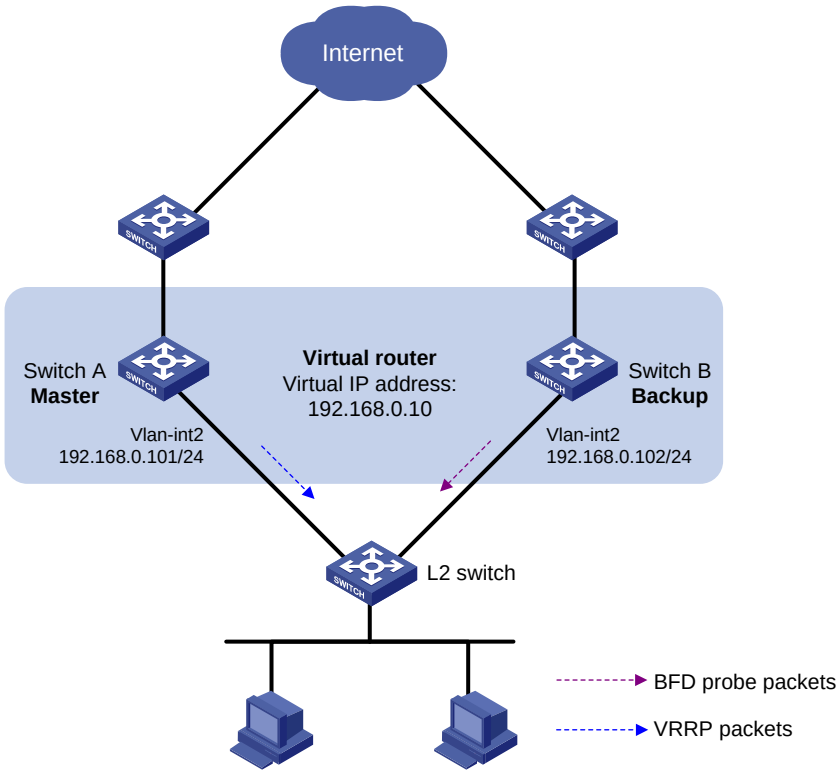
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 250, configure a VRRP group on Switch A and Switch B as the gateway for the hosts, and implement the following requirements:

- Switch A operates as the master to forward packets from the hosts to the external network. When Switch A fails, Switch B takes over to forward packets for the hosts.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 250 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid frequent role change in the VRRP group, configure a preemption delay.

For switches in the VRRP group to only process authorized packets, configure VRRP authentication.

Configuration restrictions and guidelines

When you configure BFD for a VRRP backup to monitor the master, follow these restrictions and guidelines:

- Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to the switches is also the same.
- Do not configure the local IP address and remote IP address for BFD packets as the virtual IP address of the VRRP group when you configure Track and BFD collaboration.

Configuration procedures

1. Configure the IP address of each interface as shown in Figure 250. (Details not shown.)

   This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way. (Details not shown.)

   # Configure Switch A:

   ```
   <SwitchA> system-view
   ```

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.101 255.255.255.0
```

2. Configure VRRP on Switch A:

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
   ```

   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   ```

   # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
   ```

   # Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
   [SwitchA-Vlan-interface2] return
   ```

3. Configure BFD on Switch B:

   # Specify the source IP address for BFD echo packets as **10.10.10.10**.

   ```
   <SwitchB> system-view
   [SwitchB] bfd echo-source-ip 10.10.10.10
   ```

4. Configure a track entry on Switch B:

   # Create track entry 1, which uses BFD to monitor the link between local IP address 192.168.0.102 and remote IP address 192.168.0.101 by sending BFD echo packets

   ```
   [SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local
   ip 192.168.0.102
   ```

5. Configure VRRP on Switch B:

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

   ```
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
   ```

   # Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
   ```

   # Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

   ```
   [SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
   ```

   # Configure VRRP group 1 to monitor the status of track entry 1. When the status of the track entry becomes Negative, Switch B quickly becomes the master.

   ```
   [SwitchB-Vlan-interface2] vrrp vrid 1 track 1 switchover
   [SwitchB-Vlan-interface2] return
   ```

6. Configure the hosts:

   Configure the default gateway of the hosts as **192.168.0.10**. (Details not shown.)

Verifying the configuration

Display detailed information about VRRP group 1 on Switch A.

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
```

```
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 1
     Admin Status   : Up                 State        : Master
     Config Pri     : 110                Running Pri  : 110
     Preempt Mode   : Yes                Delay Time   : 5
     Auth Type      : Simple             Key          : ******
     Virtual IP     : 192.168.0.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.101
```

Display detailed information about VRRP group 1 on Switch B.

```
<SwitchB> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 1
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Ru nning Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple             Key          : ******
     Virtual IP     : 192.168.0.10
     Master IP      : 192.168.0.101
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Switchover
```

Display information about track entry 1 on Switch B.

```
<SwitchB> display track 1
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 2 minutes 22 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 192.168.0.101
    Local IP   : 192.168.0.102
```

The output shows that when the status of the track entry becomes Positive, Switch A is the master and Switch B is the backup.

Enable VRRP state debugging and BFD event debugging on Switch B.

```
<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp state
```

```
<SwitchB> debugging bfd event
```

When Switch A or its uplink interface fails, the following output is displayed on Switch B.

```
*Dec 17 14:44:34:142 2012 SwitchB BFD/7/EVENT: Send sess-down Msg,
[Src:192.168.0.102,Dst:192.168.0.101,Vlan-interface2,Echo], instance:0, protocol:Track
*Dec 17 14:44:34:144 2012 SwitchB VRRP/7/DebugState: IPv4 Vlan-interface2 | Virtual Router
1 : Backup --> Master   reason: The status of the tracked object changed
```

Display detailed information about VRRP group 1 on Switch B.

```
<SwitchB> display vrrp verbose
IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 1
     Admin Status   : Up                 State         : Master
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : Simple             Key           : ******
     Virtual IP     : 192.168.0.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.102
   VRRP Track Information:
     Track Object   : 1                  State : Negative   Switchover
```

The output shows that when BFD detects that Switch A fails, the Track module notifies VRRP to change the status of Switch B to master immediately, without waiting for a period that is three times the advertisement interval.

Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.101 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher $c$3$Fq7Gw6ux6gf6sjUnaPxfYaJSJ08r
xGhc
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

- Switch B:

```
#
```

```
 bfd echo-source-ip 10.10.10.10
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.102 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track 1 switchover
 vrrp vrid 1 authentication-mode simple cipher $c$3$1SjZTNgoayfie8IplIGd+p1lI64Q
oDs4
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip
192.168.0.102
#
```

Example: Configuring multiple VRRP groups

Applicable product matrix

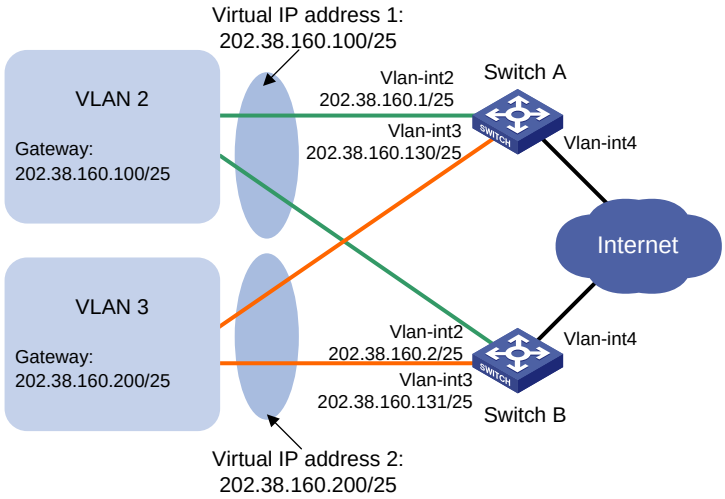
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 251, Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2, and Switch B operates as the master of VRRP group 2 to forward packets from VLAN3. When one of the switches fails, the other switch provides gateway service for both areas.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

Figure 251 Network diagram



You can configure collation between VRRP and Track, NQA, or BFD on the master to monitor the uplink status. For more information, see "Example: Configuring VRRP-Track-NQA collaboration for the master to monitor the uplinks."

You can configure BFD for a VRRP backup to monitor the master. For more information, see "Example: Configuring VRRP-Track-BFD collaboration for a backup to monitor the master."

Requirements analysis

Configure VRRP tracking on the master so that when its uplink interface fails, the master decreases its priority for the backup to take over.

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid frequent role change in the VRRP group, configure a preemption delay.

Configuration restrictions and guidelines

Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in one VRRP group. Make sure the number of virtual IP addresses assigned to the switches is also the same.

Configuration procedures

1. Configure Switch A:

   # Configure VLAN 4.

```
<SwitchA> system-view
[SwitchA] vlan 4
[SwitchA-vlan4] port gigabitethernet 1/0/7
[SwitchA-vlan4] quit
[SwitchA] interface Vlan-interface 4
[SwitchA-Vlan-interface4] ip address 20.1.1.2 255.255.255.0
[SwitchA-Vlan-interface4] quit
```

   # Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.128
```

Create VRRP group 1, and set its virtual IP address to **202.38.160.100**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
```

Assign Switch A a priority of 110 in VRRP group 1.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

In the VRRP group, track the link state of VLAN-interface 4, and specify the priority of Switch A to decrement by 30 when VLAN-interface 4 is down.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 4 reduced 30
[SwitchA-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 202.38.160.130 255.255.255.128
```

Create VRRP group 2, and set its virtual IP address to **202.38.160.200**.

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface3] vrrp vrid 2 preempt-mode timer delay 5
```

2. Configure Switch B:

Configure VLAN 4.

```
<SwitchB> system-view
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/7
[SwitchB-vlan4] quit
[SwitchB] interface Vlan-interface 4
[SwitchB-Vlan-interface4] ip address 30.1.1.2 255.255.255.0
[SwitchB-Vlan-interface4] quit
```

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.128
```

Create VRRP group 1, and set its virtual IP address to **202.38.160.100**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

```
[SwitchB-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 202.38.160.131 255.255.255.128
```

Create VRRP group 2, and set its virtual IP address to **202.38.160.200**.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

Assign Switch B a priority of 110 in VRRP group 2.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 preempt-mode timer delay 5
```

In the VRRP group, track the link state of VLAN-interface 4, and specify the priority of Switch B to decrement by 30 when VLAN-interface 4 is down.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 track interface vlan-interface 4 reduced 30
```

3. Configure the hosts:

   Configure the default gateway of the hosts in VLAN 2 as **202.38.160.100/25** and in VLAN 3 as **202.38.160.200/25**. (Details not shown.)

Verifying the configuration

Display detailed information about the VRRP groups on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 1
     Admin Status   : Up                State         : Master
     Config Pri     : 110               Running Pri   : 110
     Preempt Mode   : Yes               Delay Time    : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Virtual MAC    : 0000-5e00-011e
     Master IP      : 202.38.160.1
     VRRP Track Information:
     Track Interface: Vlan4         State : Up              Pri Reduced : 30

   Interface Vlan-interface3
     VRID           : 2                 Adver Timer   : 1
     Admin Status   : Up                State         : Backup
     Config Pri     : 100               Running Pri   : 100
     Preempt Mode   : Yes               Delay Time    : 5
     Become Master  : 2200ms left
     Auth Type      : None
```

```
    Virtual IP     : 202.38.160.200
    Master IP      : 202.38.160.131
```

Display detailed information about the VRRP groups on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 1
     Admin Status   : Up                State         : Backup
     Config Pri     : 100               Running Pri   : 100
     Preempt Mode   : Yes               Delay Time    : 5
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Master IP      : 202.38.160.1

   Interface Vlan-interface3
     VRID           : 2                 Adver Timer   : 1
     Admin Status   : Up                State         : Master
     Config Pri     : 110               Running Pri   : 110
     Preempt Mode   : Yes               Delay Time    : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.200
     Virtual MAC    : 0000-5e00-0120
     Master IP      : 202.38.160.131
     VRRP Track Information:
     Track Interface: Vlan4         State : Up              Pri Reduced : 30
```

The output shows the following:

- Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 202.38.160.100/25.
- Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 202.38.160.200/25.

Display detailed information about VRRP group 1 on Switch B when Switch A fails.

```
[SwitchB-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 1
     Admin Status   : Up                State         : Master
     Config Pri     : 100               Running Pri   : 100
     Preempt Mode   : Yes               Delay Time    : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.100
```

```
  Virtual MAC     : 0000-5e00-011e
  Master IP       : 202.38.160.2

Interface Vlan-interface3
  VRID            : 2                   Adver Timer   : 1
  Admin Status    : Up                  State         : Master
  Config Pri      : 110                 Running Pri   : 110
  Preempt Mode    : Yes                 Delay Time    : 5
  Auth Type       : None
  Virtual IP      : 202.38.160.200
  Virtual MAC     : 0000-5e00-0120
  Master IP       : 202.38.160.131
  VRRP Track Information:
  Track Interface: Vlan4         State : Up                Pri Reduced : 30
```

The output shows that when Switch A fails, Switch B operates as the master in VRRP group 1 to forward Internet traffic for hosts in VLAN 2.

Configuration files

- Switch A:

```
#
vlan 2 to 4
#
interface Vlan-interface2
 ip address 202.38.160.1 255.255.255.128
 vrrp vrid 1 virtual-ip 202.38.160.100
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track interface vlan-interface4 reduced 30
#
interface Vlan-interface3
 ip address 202.38.160.130 255.255.255.128
 vrrp vrid 2 virtual-ip 202.38.160.200
 vrrp vrid 2 preempt-mode timer delay 5
#
interface Vlan-interface4
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#
```

- Switch B:

```
#
vlan 2 to 4
#
interface Vlan-interface2
 ip address 202.38.160.2 255.255.255.128
 vrrp vrid 1 virtual-ip 202.38.160.100
 vrrp vrid 1 preempt-mode timer delay 5
#
interface Vlan-interface3
 ip address 202.38.160.131 255.255.255.128
 vrrp vrid 2 virtual-ip 202.38.160.200
 vrrp vrid 2 priority 110
 vrrp vrid 2 preempt-mode timer delay 5
 vrrp vrid 2 track interface vlan-interface4 reduced 30
#
interface Vlan-interface4
 ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#
```

Example: Using VRRP with MSTP

Applicable product matrix

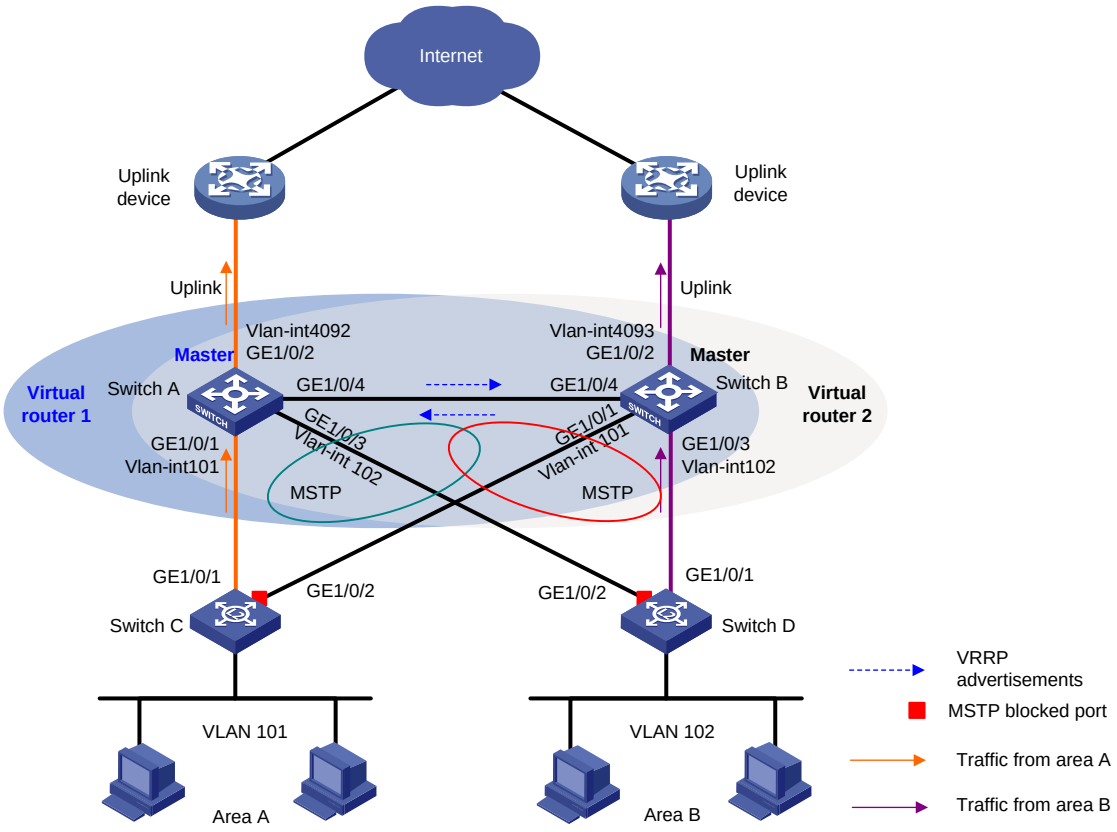
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 252, Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2, and Switch B operates as the master of VRRP group 2 to forward packets from VLAN3. When one of the switches fails, the other switch provides gateway service for both VLANs.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

Figure 252 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

Configure VRRP tracking on the master so that when its uplink is not available, the master decreases its priority for the backup to take over.

To avoid loops between Switch A, Switch B, Switch C, and Switch D, enable MSTP on them.

Configuration procedures

1. Configure Switch A:

   # Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4092.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] port gigabitethernet 1/0/1
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port gigabitethernet 1/0/3
[SwitchA-vlan102] quit
[SwitchA] vlan 4092
[SwitchA-vlan4092] port gigabitethernet 1/0/2
[SwitchA-vlan4092] quit
```

Configure GigabitEthernet 1/0/4 as a trunk port, remove the port from VLAN 1, and assign the port to VLAN 101 and VLAN 102.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchA-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchA-GigabitEthernet1/0/4] quit
```

Configure the uplink interface.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] undo stp enable
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface vlan-interface 4092
[SwitchA-Vlan-interface4092] ip address 10.1.1.2 24
```

On VLAN-interface 101, create VRRP group 1, assign virtual IP address **10.10.101.1** to the VRRP group, and assign a priority of 110 to the switch in the VRRP group.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ip address 10.10.101.2 24
[SwitchA-Vlan-interface101] vrrp vrid 1 virtual-ip 10.10.101.1
[SwitchA-Vlan-interface101] vrrp vrid 1 priority 110
```

In the VRRP group, track VLAN-interface 4092, and specify the priority of Switch A to decrease by 20 when VLAN-interface 4092 becomes unavailable.

```
[SwitchA-Vlan-interface101] vrrp vrid 1 track interface Vlan-interface4092 reduced
20
[SwitchA-Vlan-interface101] quit
```

Create VRRP group 2.

```
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ip address 10.10.102.2 24
[SwitchA-Vlan-interface102] vrrp vrid 1 virtual-ip 10.10.102.1
[SwitchA–Vlan-interface102] quit
```

Configure MSTP.

```
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name vrrp
[SwitchA-mst-region] instance 1 vlan 101
[SwitchA-mst-region] instance 2 vlan 102
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
[SwitchA] stp instance 1 root primary
[SwitchA] stp instance 2 root secondary
[SwitchA] stp enable
```

2. Configure Switch B:

Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4093.

```
<SwitchB> system-view
[SwitchB] vlan 101
[SwitchB-vlan101] port gigabitethernet 1/0/1
[SwitchB-vlan101] quit
```

```
[SwitchB] vlan 102
[SwitchB-vlan102] port gigabitethernet 1/0/3
[SwitchB-vlan102] quit
[SwitchB] vlan 4093
[SwitchB-vlan4093] port gigabitethernet 1/0/2
[SwitchB-vlan4093] quit
```

Configure GigabitEthernet 1/0/4 as a trunk port, remove the port from VLAN 1, and assign the port to VLAN 101 and VLAN 102.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchB-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure the uplink interface.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] undo stp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface vlan-interface 4093
[SwitchB-Vlan-interface4093] ip address 10.1.2.2 24
```

Create VRRP group 1.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 10.10.101.3 24
[SwitchB-Vlan-interface101] vrrp vrid 1 virtual-ip 10.10.101.1
[SwitchB–Vlan-interface101] quit
```

Create VRRP group 2 and assign virtual IP address **10.10.102.1** to the VRRP group, and assign a priority of **110** to the switch in the VRRP group.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] ip address 10.10.102.3 24
[SwitchB-Vlan-interface102] vrrp vrid 1 virtual-ip 10.10.102.1
[SwitchB-Vlan-interface102] vrrp vrid 1 priority 110
```

In the VRRP group, track VLAN-interface 4093, and specify the priority of Switch B to decrease by 20 when VLAN-interface 4093 becomes unavailable.

```
[SwitchB-Vlan-interface102] vrrp vrid 1 track interface Vlan-interface4093 reduced
20
[SwitchB-Vlan-interface102] quit
```

Configure MSTP.

```
[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name vrrp
[SwitchB-mst-region] instance 1 vlan 101
[SwitchB-mst-region] instance 2 vlan 102
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
[SwitchB] stp instance 2 root primary
[SwitchB] stp instance 1 root secondary
[SwitchB] stp enable
```

3. Configure Switch C:

Configure VLAN 101.

```
<SwitchC> system-view
[SwitchC] vlan 101
[SwitchC-vlan101] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchC-vlan101] quit
```

Configure MSTP.

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] region-name vrrp
[SwitchC-mst-region] instance 1 vlan 101
[SwitchC-mst-region] instance 2 vlan 102
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
[SwitchC] stp enable
```

4. Configure Switch D:

Configure VLAN 102.

```
<SwitchD> system-view
[SwitchD] vlan 102
[SwitchD-vlan102] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchD-vlan102] quit
```

Configure MSTP.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] region-name vrrp
[SwitchD-mst-region] instance 1 vlan 101
[SwitchD-mst-region] instance 2 vlan 102
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
[SwitchD] stp enable
```

5. Configure the hosts:

   Configure the default gateway 10.10.101.1 for hosts in area A and 10.10.102.1 for hosts in a area B. (Details not shown.)

Verifying the configuration

Execute the **display vrrp verbose** command to display detailed information about the VRRP, and execute the **display stp brief** command to display brief information about MSTP.

Configuration files

- Switch A:

```
#
 vlan 101 to 102
#
 vlan 4092
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
```

```
 active region-configuration
#
 stp instance 1 root primary
 stp instance 2 root secondary
 stp enable
#
interface Vlan-interface101
 ip address 10.10.101.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.10.101.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 track interface Vlan-interface4092 reduced 20
#
interface Vlan-interface102
 ip address 10.10.102.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.10.102.1
#
interface Vlan-interface4092
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 4092
#
interface GigabitEthernet1/0/3
 port access vlan 102
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
```

- Switch B:

```
#
 vlan 101 to 102
#
 vlan 4093
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp instance 1 root secondary
 stp instance 2 root primary
```

```
 stp enable
#
interface Vlan-interface101
 ip address 10.10.101.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.10.101.1
#
interface Vlan-interface102
 ip address 10.10.102.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.10.102.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 track interface Vlan-interface4093 reduced 20
#
interface Vlan-interface4093
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 4093
#
interface GigabitEthernet1/0/3
 port access vlan 102
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
```

- Switch C:

```
#
 vlan 101
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 101
#
```

- Switch D:

```
#
 vlan 102
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port access vlan 102
#
interface GigabitEthernet1/0/2
 port access vlan 102
#
```

IPv6-based VRRP configuration examples

This chapter provides IPv6-based VRRP configuration examples.

Example: Configuring a single VRRP group

Applicable product matrix

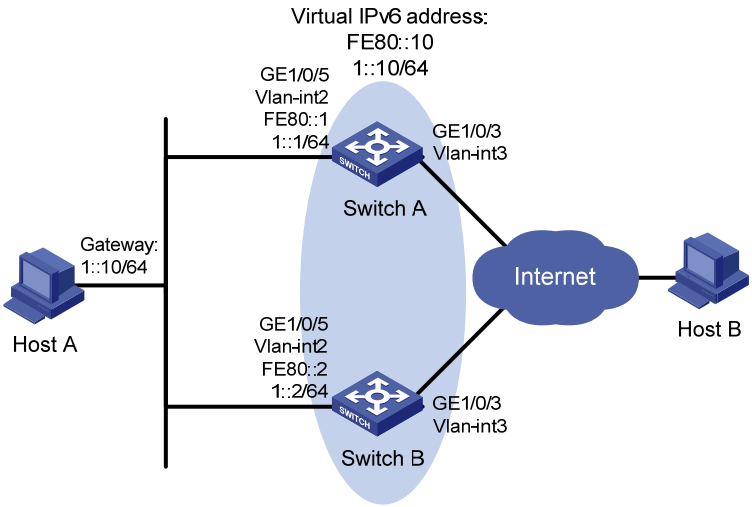
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 253, configure a VRRP group on Switch A and Switch B as the gateway for the hosts, and implement the following requirements:

- Switch A operates as the master to forward packets from the hosts to the external network. When Switch A fails, Switch B takes over to forward packets for the hosts.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 253 Network diagram



Requirements analysis

- For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.
- Configure VRRP tracking on Switch A so that when its uplink is not available, Switch A decreases its priority for Switch B to take over quickly.
- To avoid frequent role change in the VRRP group, configure a preemption delay.
- For switches in the VRRP group to only process authorized packets, configure VRRP authentication.

Configuration procedures

1. Configure Switch A:

   # Enable IPv6 globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6
   ```

   # Configure VLAN 3.

   ```
   [SwitchA] vlan 3
   [SwitchA-vlan3] port gigabitethernet 1/0/3
   [SwitchA-vlan3] quit
   [SwitchA] interface vlan-interface 3
   [SwitchA-Vlan-interface3] ipv6 address 2003::2 64
   [SwitchA-Vlan-interface3] quit
   ```

   # Configure VLAN 2.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   ```

   # Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```

Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly, and set the preemption delay to 5 seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

In the VRRP group, track the link state of VLAN-interface 3, and specify the priority of Switch A to decrement by 30 when VLAN-interface 3 is down.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 3 reduced
30
```

Enable Switch A to send RA messages, so Host A can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

2. Configure Switch B:

Enable IPv6 globally.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address 2004::2 64
[SwitchB-Vlan-interface3] quit
```

Configure VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```

Configure Switch B to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5 seconds to avoid frequent status switchover.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

Enable Switch B to send RA messages, so Host A can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

3. Configure the hosts:

Configure the default gateway of Host A as 1::10/64. (Details not shown.)

Verifying the configuration

Ping Host B from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 110                Running Pri   : 110
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : Simple             Key           : ******
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Interface: Vlan3               State : Up         Pri Reduced : 30
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Backup
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Become Master  : 3600ms left
     Auth Type      : Simple             Key           : ******
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

Ping Host B from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
```

```
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Backup
     Config Pri     : 110                Running Pri   : 80
     Preempt Mode   : Yes                Delay Time    : 5
     Become Master  : 3600ms left
     Auth Type      : Simple             Key           : ******
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::2
   VRRP Track Information:
     Track Interface: Vlan3              State : Down       Pri Reduced : 30
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : Simple             Key           : ******
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::2
```

The output shows that when VLAN-interface 3 on Switch A is not available, the priority of Switch A is reduced to 80 and it becomes the backup. Switch B becomes the master to forward packets from Host A to Host B.

Configuration files

- Switch A:

```
#
 ipv6
#
 vlan 2 to 3
#
interface Vlan-interface2
 undo ipv6 nd ra halt
 ipv6 address 1::1 64
 ipv6 address FE80::1 link-local vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 110
 vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

```
 vrrp ipv6 vrid 1 track interface vlan-interface3 reduced 30
 vrrp ipv6 vrid 1 authentication-mode simple cipher $c$3$bGi6EvJRLUqCKHO7yY9RlrA
hcMFWhyzz
#
interface Vlan-interface3
 ipv6 address 2003::2/64
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

- Switch B:

```
#
 ipv6
#
 vlan 2 to 3
#
interface Vlan-interface2
 undo ipv6 nd ra halt
 ipv6 address 1::2 64
 ipv6 address FE80::2 link-local
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode timer delay 5
 vrrp ipv6 vrid 1 authentication-mode simple cipher $c$3$IL0Gzf/m1E/Hn8eGeniH+LW
KHpeAjCyX
#
interface Vlan-interface3
 ipv6 address 2004::2/64
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring multiple VRRPv3 groups

Applicable product matrix

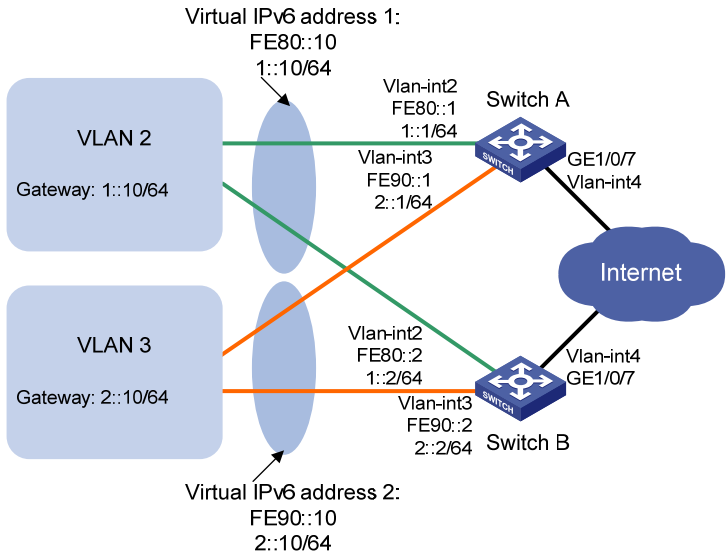
Product series	Software version
HP 7500	Release series 6620 Release series 6630 Release series 6700

Network requirements

As shown in Figure 254, Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from Area A, and Switch B operates as the master of VRRP group 2 to forward packets from Area B. When one of the switches fails, the other switch provides gateway service for both areas.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

Figure 254 Network diagram



Requirements analysis

- For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.
- Configure VRRP tracking on Switch A so that when its uplink is not available, Switch A decreases its priority for Switch B to take over quickly.
- To avoid frequent role change in the VRRP group, configure a preemption delay.

Configuration restrictions and guidelines

When you configure multiple VRRP groups, follow these restrictions and guidelines:

- Configure a default gateway to implement VRRP load balancing.
- Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in one VRRP group. Make sure the number of virtual IP addresses assigned to the switches is also the same.

Configuration procedures

1. Configure Switch A:

   # Enable IPv6 globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6
   ```

   # Configure VLAN 4.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 4
   [SwitchA-vlan4] port gigabitethernet 1/0/7
   [SwitchA-vlan4] quit
   [SwitchA] interface Vlan-interface 4
   [SwitchA-Vlan-interface4] ipv6 address 2000::2 64
   [SwitchA-Vlan-interface4] quit
   ```

   # Configure VLAN 2.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   ```

   # Create VRRP group 1, and set its virtual IP addresses to **FE80::10** and **1::10**.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
   ```

   # Assign Switch A a priority of 110 in VRRP group 1.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
   ```

   # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
   ```

   # In the VRRP group, track the link state of VLAN-interface 4, and specify the priority of Switch A to decrement by 30 when VLAN-interface 4 is down.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 4 reduced
   30
   ```

   # Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

   ```
   [SwitchA-Vlan-interface2] undo ipv6 nd ra halt
   [SwitchA-Vlan-interface2] quit
   ```

   # Configure VLAN 3.

   ```
   [SwitchA] vlan 3
   ```

```
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
[SwitchA-Vlan-interface3] ipv6 address 2::1 64
```

Create VRRP group 2, and set its virtual IP addresses to **FE90::10** and **2::10**.

```
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 preempt-mode timer delay 5
```

Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

```
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

2. Configure Switch B:

Enable IPv6 globally.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Configure VLAN 4.

```
<SwitchB> system-view
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/7
[SwitchB-vlan4] quit
[SwitchB] interface Vlan-interface 4
[SwitchB-Vlan-interface4] ipv6 address 2001::2 64
[SwitchB-Vlan-interface4] quit
```

Configure VLAN 2.

```
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

Create VRRP group 1, and set its virtual IP addresses to **FE80::10** and **1::10**.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
```

```
[SwitchB-Vlan-interface3] ipv6 address 2::2 64
```

Create VRRP group 2, and set its virtual IP address to **FE90::10** and **2::10**.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

Assign Switch B a priority of 110 in VRRP group 2.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 preempt-mode timer delay 5
```

In the VRRP group, track the link state of VLAN-interface 4, and specify the priority of Switch B to decrement by 30 when VLAN-interface 4 is down.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 track interface vlan-interface 4 reduced
30
```

Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

```
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

3. Configure the hosts:

   Configure the default gateway of the hosts in VLAN 2 as **1::10/64** and in VLAN 3 as **2::10/64**. (Details not shown.)

Verifying the configuration

Display detailed information about the VRRP groups on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 110                Running Pri   : 110
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Interface: Vlan4          State : Up               Pri Reduced : 30

   Interface Vlan-interface3
     VRID           : 2                  Adver Timer   : 100
     Admin Status   : Up                 State         : Backup
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Become Master  : 3600ms left
     Auth Type      : None
```

```
    Virtual IP     : FE90::10
                     2::10
    Master IP      : FE90::2
```

Display detailed information about the VRRP groups on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
 IPv6 Standby Information:
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Backup
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 5
     Become Master  : 3600ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1

   Interface Vlan-interface3
     VRID           : 2                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 110                Running Pri   : 110
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : None
     Virtual IP     : FE90::10
                      2::10
     Virtual MAC    : 0000-5e00-0202
     Master IP      : FE90::2
   VRRP Track Information:
     Track Interface: Vlan4          State : Up               Pri Reduced : 30
```

The output shows the following:

- Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 1::10/64.
- Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 2::10/64.

Display detailed information about VRRP group 1 on Switch B when Switch A fails.

```
 [SwitchB-Vlan-interface3] display vrrp ipv6 verbose
 IPv6 Standby Information:
    Run Mode       : Standard
    Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 100                Running Pri   : 100
```

```
  Preempt Mode   : Yes                 Delay Time   : 5
  Auth Type      : None
  Virtual IP     : FE80::10
                   1::10
  Virtual MAC    : 0000-5e00-0201
  Master IP      : FE80::2
Interface Vlan-interface3
  VRID           : 2                   Adver Timer  : 100
  Admin Status   : Up                  State        : Master
  Config Pri     : 110                 Running Pri  : 110
  Preempt Mode   : Yes                 Delay Time   : 5
  Auth Type      : None
  Virtual IP     : FE90::10
                   2::10
  Virtual MAC    : 0000-5e00-0202
  Master IP      : FE90::2
VRRP Track Information:
  Track Interface: Vlan4          State : Up               Pri Reduced : 30
```

The output shows that when Switch A fails, Switch B operates as the master in VRRP group 1 to forward Internet traffic for hosts in VLAN 2.

Configuration files

- Switch A:

```
#
 ipv6
#
 vlan 2 to 4
#
interface Vlan-interface2
 undo ipv6 nd ra halt
 ipv6 address 1::1 64
 ipv6 address FE80::1 link-local
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 110
 vrrp ipv6 vrid 1 preempt-mode timer delay 5
 vrrp ipv6 vrid 1 track interface vlan-interface4 reduced 30
#
interface Vlan-interface3
 undo ipv6 nd ra halt
 ipv6 address 2::1 64
 ipv6 address FE90::1 link-local
 vrrp ipv6 vrid 2 virtual-ip FE90::10 link-local
 vrrp ipv6 vrid 2 virtual-ip 2::10
 vrrp ipv6 vrid 2 preempt-mode timer delay 5
#
interface Vlan-interface4
```

```
 ipv6 address 2000::2/64
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#
```

- Switch B:

```
#
 ipv6
#
 vlan 2 to 4
#
interface Vlan-interface2
 undo ipv6 nd ra halt
 ipv6 address 1::2 64
 ipv6 address FE80::2 link-local
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode timer delay 5
#
interface Vlan-interface3
 undo ipv6 nd ra halt
 ipv6 address 2::2 64
 ipv6 address FE90::2 link-local
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 2 virtual-ip FE90::20 link-local
 vrrp ipv6 vrid 2 virtual-ip 2::10
 vrrp ipv6 vrid 2 priority 110
 vrrp ipv6 vrid 2 preempt-mode timer delay 5
 vrrp ipv6 vrid 2 track interface vlan-interface4 reduced 30
#
interface Vlan-interface4
 ipv6 address 2001::2/64
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#
```

Example: Using VRRPv3 with MSTP

Applicable product matrix

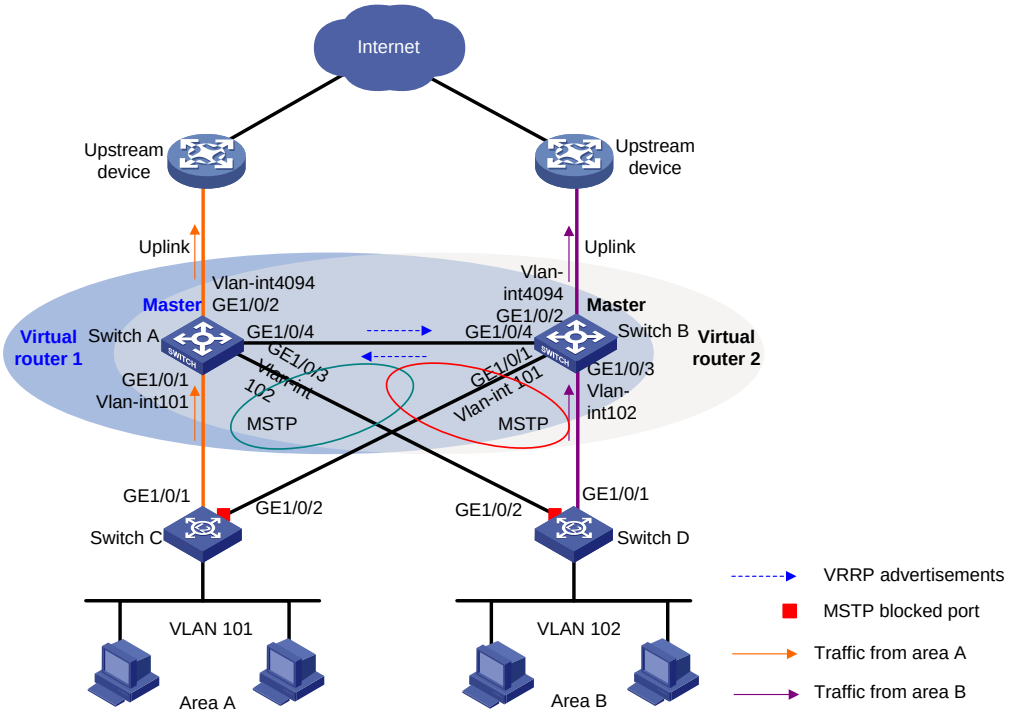
Product series	Software version
HP 7500	Release series 6620
	Release series 6630
	Release series 6700

Network requirements

As shown in Figure 255, Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2, and Switch B operates as the master of VRRP group 2 to forward packets from VLAN3. When one of the switches fails, the other switch provides gateway service for both VLANs.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

Figure 255 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

Configure VRRP tracking on the master so that when its uplink is not available, the master decreases its priority for the backup to take over.

To avoid loops between Switch A, Switch B, Switch C, and Switch D, enable MSTP on them.

Configuration procedures

1. Configure Switch A:

   # Enable IPv6 globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6
   ```

   # Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4092.

   ```
   [SwitchA] vlan 101
   [SwitchA-vlan101] port gigabitethernet 1/0/1
   [SwitchA-vlan101] quit
   [SwitchA] vlan 102
   [SwitchA-vlan102] port gigabitethernet 1/0/3
   [SwitchA-vlan102] quit
   [SwitchA] vlan 4092
   [SwitchA-vlan4092] port gigabitethernet 1/0/2
   [SwitchA-vlan4092] quit
   ```

   # Configure GigabitEthernet 1/0/4 as a trunk port, remove the port from VLAN 1, and assign the port to VLAN 101 and VLAN 102.

   ```
   [SwitchA] interface gigabitethernet 1/0/4
   [SwitchA-GigabitEthernet1/0/4] port link-type trunk
   [SwitchA-GigabitEthernet1/0/4] undo port trunk permit vlan 1
   [SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
   [SwitchA-GigabitEthernet1/0/4] port trunk pvid vlan 101
   [SwitchA-GigabitEthernet1/0/4] quit
   ```

   # Configure the uplink interface.

   ```
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] undo stp enable
   [SwitchA-GigabitEthernet1/0/2] quit
   [SwitchA] interface vlan-interface 4092
   [SwitchA-Vlan-interface4092] ipv6 address 2003::2 64
   ```

   # Create VRRP group 1.

   ```
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] ipv6 address fe80::2 link-local
   [SwitchA-Vlan-interface101] ipv6 address 2001::2 64
   [SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
   [SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip 2001::1
   ```

   # Configure the priority of VRRP group 1 as **110**.

   ```
   [SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 priority 110
   ```

   # In the VRRP group, track VLAN-interface 4092, and specify the priority of Switch A to decrease by 20 when VLAN-interface 4092 becomes unavailable.

```
[SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 track interface Vlan-interface 4092
reduced 20
```

Enable Switch A to send RA messages, so the hosts can learn the default gateway address.

```
[SwitchA-Vlan-interface101] undo ipv6 nd ra halt
[SwitchA-Vlan-interface101] quit
```

Create VRRP group 2.

```
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ipv6 address fe90::2 link-local
[SwitchA-Vlan-interface102] ipv6 address 2002::2 64
[SwitchA-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip FE90::1 link-local
[SwitchA-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip 2002::1
```

Enable Switch A to send RA messages, so the hosts can learn the default gateway address.

```
[SwitchA-Vlan-interface102] undo ipv6 nd ra halt
[SwitchA-Vlan-interface102] quit
```

Configure MSTP.

```
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name vrrp
[SwitchA-mst-region] instance 1 vlan 101
[SwitchA-mst-region] instance 2 vlan 102
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
[SwitchA] stp instance 1 root primary
[SwitchA] stp instance 2 root secondary
[SwitchA] stp enable
```

2. Configure Switch B:

Enable IPv6 globally.

```
<SwitchB> system-view
[SwitchB] ipv6
```

Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4093.

```
[SwitchB] vlan 101
[SwitchB-vlan101] port gigabitethernet 1/0/1
[SwitchB-vlan101] quit
[SwitchB] vlan 102
[SwitchB-vlan102] port gigabitethernet 1/0/3
[SwitchB-vlan102] quit
[SwitchB] vlan 4093
[SwitchB-vlan4093] port gigabitethernet 1/0/2
[SwitchB-vlan4093] quit
```

Configure GigabitEthernet 1/0/4 as a trunk port, remove the port from VLAN 1, and assign the port to VLAN 101 and VLAN 102.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchB-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure the uplink interface.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] undo stp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface vlan-interface 4093
[SwitchB-Vlan-interface4093] ipv6 address 2004::2 64
```

Create VRRP group 1.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address fe80::3 link-local
[SwitchB-Vlan-interface101] ipv6 address 2001::3 64
[SwitchB-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
[SwitchB-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip 2001::1
```

Create VRRP group 2.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] ipv6 address fe90::3 link-local
[SwitchB-Vlan-interface102] ipv6 address 2002::3 64
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip FE90::1 link-local
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip 2002::1
```

Configure the priority of VRRP group 2 as **110**.

```
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 priority 110
```

In the VRRP group, track VLAN-interface 4093, and specify the priority of Switch B to decrease by 20 when VLAN-interface 4093 becomes unavailable.

```
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 track interface Vlan-interface 4093
reduced 20
```

Enable Switch B to send RA messages, so the hosts can learn the default gateway address.

```
[SwitchB-Vlan-interface102] undo ipv6 nd ra halt
[SwitchB-Vlan-interface102] quit
```

Configure MSTP.

```
[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name vrrp
[SwitchB-mst-region] instance 1 vlan 101
[SwitchB-mst-region] instance 2 vlan 102
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
[SwitchB] stp instance 2 root primary
[SwitchB] stp instance 1 root secondary
[SwitchB] stp enable
```

3. Configure Switch C:

Configure VLAN 101.

```
<SwitchC> system-view
[SwitchC] vlan 101
[SwitchC-vlan101] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchC-vlan101] quit
```

Configure MSTP.

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] region-name vrrp
[SwitchC-mst-region] instance 1 vlan 101
```

```
[SwitchC-mst-region] instance 2 vlan 102
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
[SwitchC] stp enable
```

4. Configure Switch D:

   # Configure VLAN 102.

```
<SwitchD> system-view
[SwitchD] vlan 102
[SwitchD-vlan102] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchD-vlan102] quit
```

   # Configure MSTP.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] region-name vrrp
[SwitchD-mst-region] instance 1 vlan 101
[SwitchD-mst-region] instance 2 vlan 102
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
[SwitchD] stp enable
```

5. Configure the hosts:

   Configure the default gateway 2001::1 for hosts in area A and 2002::1 for hosts in a area B. (Details not shown.)

Verifying the configuration

Execute the **display vrrp ipv6 verbose** command to display detailed information about the VRRP groups, and execute the **display stp brief** command to display brief information about MSTP.

Configuration files

- Switch A:

```
#
 ipv6
#
 vlan 101 to 102
#
 vlan 4092
#

stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp instance 1 root primary
 stp instance 2 root secondary
 stp enable
#
```

```
interface Vlan-interface101
 undo ipv6 nd ra halt
 ipv6 address 2001::2/64
 ipv6 address FE80::2 link-local
 vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
 vrrp ipv6 vrid 1 virtual-ip 2001::1
 vrrp ipv6 vrid 1 priority 110
 vrrp ipv6 vrid 1 track interface Vlan-interface4092 reduced 20
#
interface Vlan-interface102
 undo ipv6 nd ra halt
 ipv6 address 2002::2 64
 ipv6 address FE90::2 link-local
 vrrp ipv6 vrid 1 virtual-ip FE90::1 link-local
 vrrp ipv6 vrid 1 virtual-ip 2002::1
#
interface Vlan-interface4092
 ipv6 address 2003::2/64
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 4092
 stp disable
#
interface GigabitEthernet1/0/3
 port access vlan 102
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
```

- Switch B:

```
#
 ipv6
#
 vlan 101 to 102
#
 vlan 4093
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
```

```
#
 stp instance 1 root secondary
 stp instance 2 root primary
 stp enable
#
interface Vlan-interface101
 undo ipv6 nd ra halt
 ipv6 address 2001::3 64
 ipv6 address FE80::3 link-local

 vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
 vrrp ipv6 vrid 1 virtual-ip 2001::1
#
interface Vlan-interface102
 undo ipv6 nd ra halt
 ipv6 address 2002::3 64
 ipv6 address FE90::3 link-local
 vrrp ipv6 vrid 2 virtual-ip FE90::1 link-local
 vrrp ipv6 vrid 1 virtual-ip 2002::1
 vrrp ipv6 vrid 2 priority 110
 vrrp ipv6 vrid 1 track interface Vlan-interface4093 reduced 20
#
interface Vlan-interface4093
 ipv6 address 2004::2/64
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 4093
 stp disable
#
interface GigabitEthernet1/0/3
 port access vlan 102
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
```

- Switch C:

```
#
 vlan 101
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
```

```
 instance 2 vlan 102
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 101
#
```

- Switch D:

```
#
 vlan 102
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port access vlan 102
#
interface GigabitEthernet1/0/2
 port access vlan 102
    #
```