HP 5920 & 5900 Switch Series Configuration Examples

Part number: 5998 5574

Contents

802.1X configuration examples

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

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

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

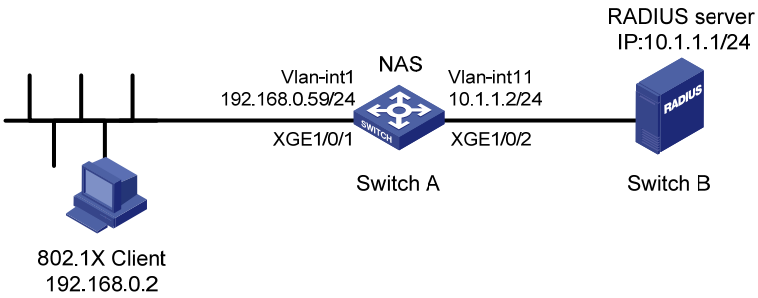
Network requirements

As shown in Figure 1, users must pass 802.1X authentication to access the Internet. 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 RADIUS server is an HP 5500 HI switch that runs Comware V5 software image.

Configure Ten-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:

- Specify the authentication port as **1645** in the RADIUS scheme on the access device when an HP device functions as the RADIUS authentication server.
- 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
   ```

   # Specify the RADIUS server at **10.1.1.1** as the primary authentication server. Set the authentication port to **1645**. Specify the shared key as **abc**.

   ```
   [SwitchA-radius-radius1] primary authentication 10.1.1.1 1645 key simple 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. For example, if the RADIUS server includes the ISP domain name in the username, the access device must also include the ISP domain name.

   # 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
   ```

   # Configure ISP domain **test** to use RADIUS scheme **radius1** for authentication and authorization of all LAN 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 Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] dot1x
   ```

   # Configure Ten-GigabitEthernet 1/0/1 to implement MAC-based access control. By default, the port implements MAC-based access control.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] dot1x port-method macbased
   ```

```
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable 802.1X globally.

```
[SwitchA] dot1x
```

Configuring the RADIUS server

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

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

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

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

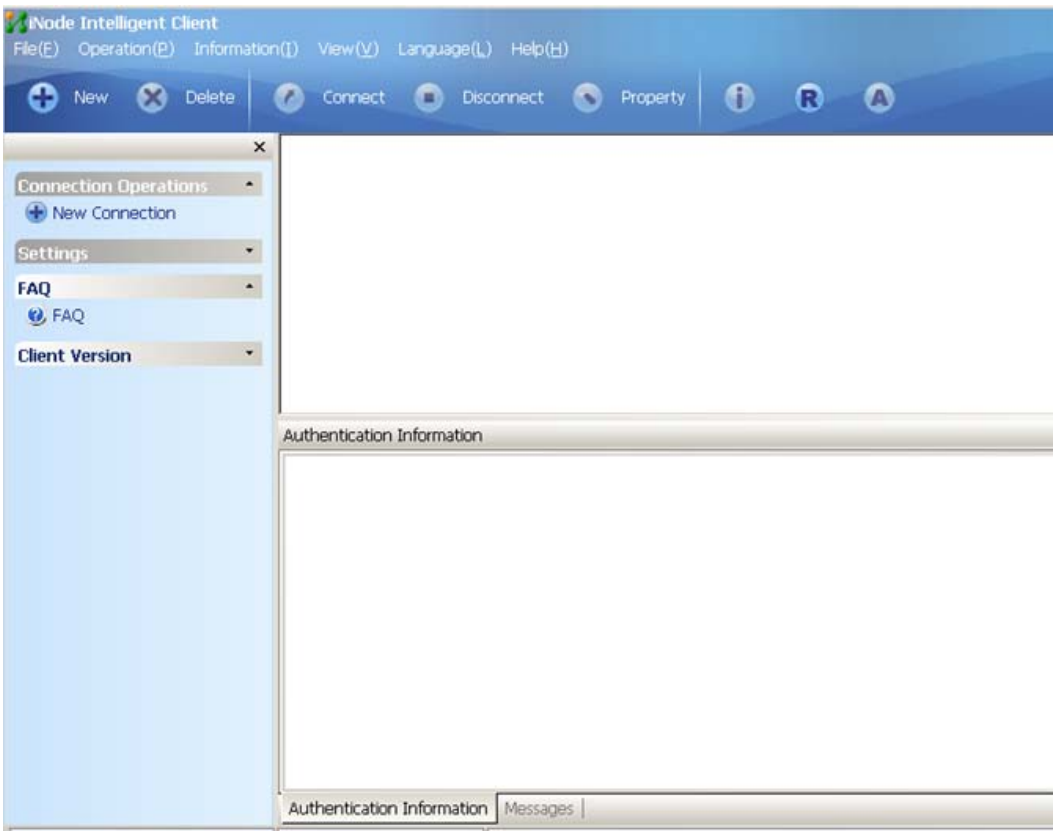
Specify RADIUS client **10.1.1.2**, and set the shared key to **abc** in plain text.

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

Configuring the 802.1X client

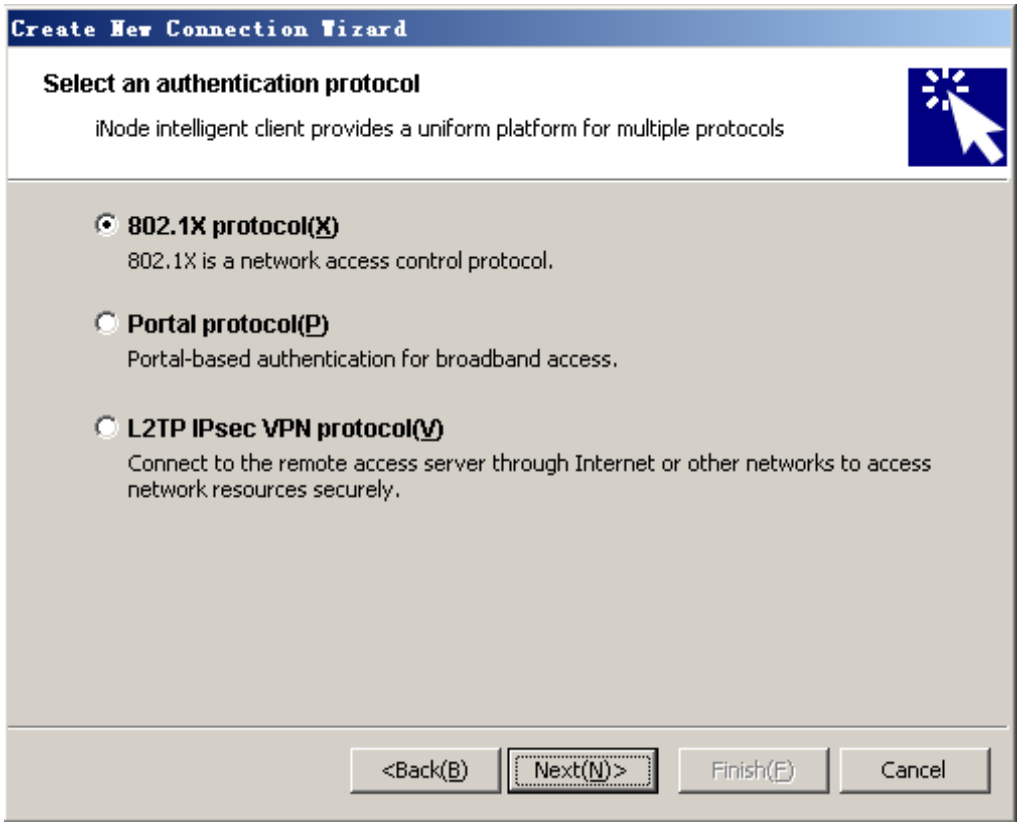
1. Open the iNode client as shown in Figure 2.

Figure 2 Opening the iNode client



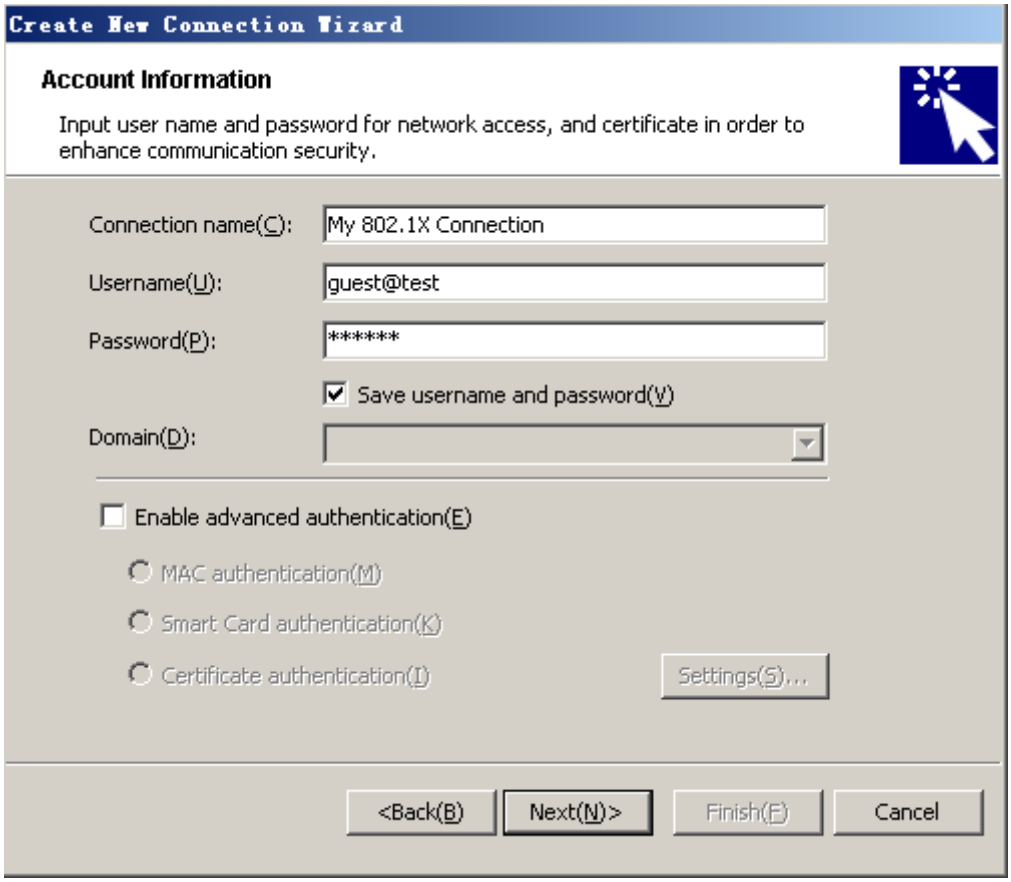
2. Click **New**.
3. On the **Create New Connection Wizard** window, select **802.1X protocol**, and then click **Next**.

Figure 3 Creating a new connection



4. Configure the connection name, username, and password, and then click **Next**.

Figure 4 Configuring the connection name, username, and password



For authentication to be performed correctly, the following details must comply with the correlation rules shown in Table 1:

- Username specified on the iNode client.
- Domain and username format configuration on the access device.
- Service suffix on UAM.

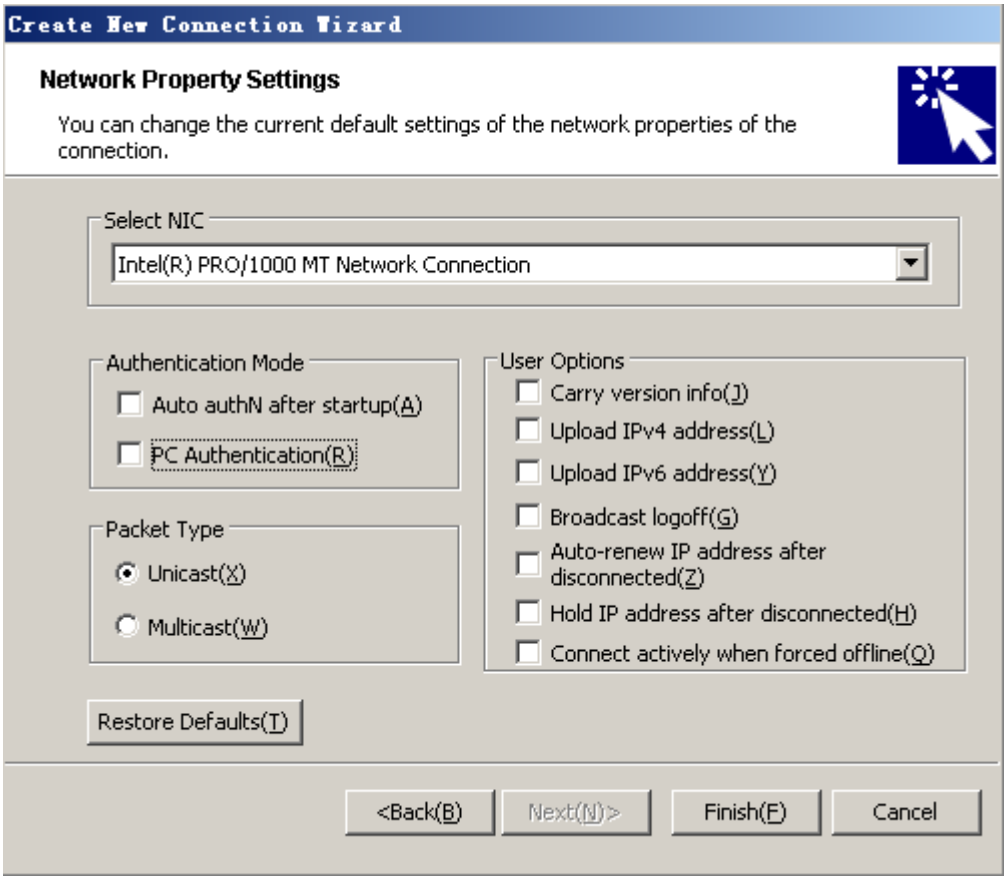
Table 1 Parameter correlation

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 network property settings.

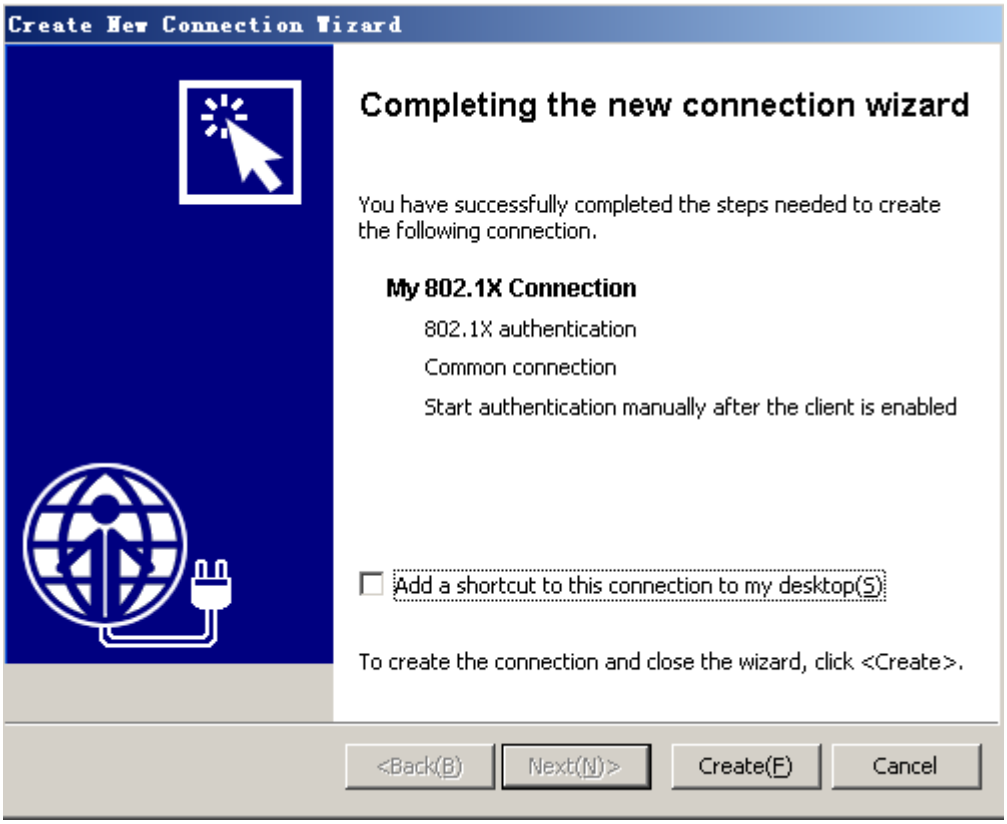
If you set local authentication as the backup authentication method, do not select **Carry version info(J)** in the **User Options** area. The access device cannot recognize the version number carried in EAP packets.

Figure 5 Configuring 802.1X connection properties



6. Click **Create**.

Figure 6 Completing the new connection wizard



Verifying the configuration

Verify that you can use the user account to pass 802.1X authentication:

Double-click **My 802.1X Connection** on the iNode client.

On the **My 802.1X Connection** window, enter username **guest@test** and password **123456**.

Click **Connect**.

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
#
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 Ten-GigabitEthernet1/0/1
```

```
 dot1x
#
interface Ten-GigabitEthernet1/0/2
 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 Ten-GigabitEthernet1/1/2
 port access vlan 11
#
```

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

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

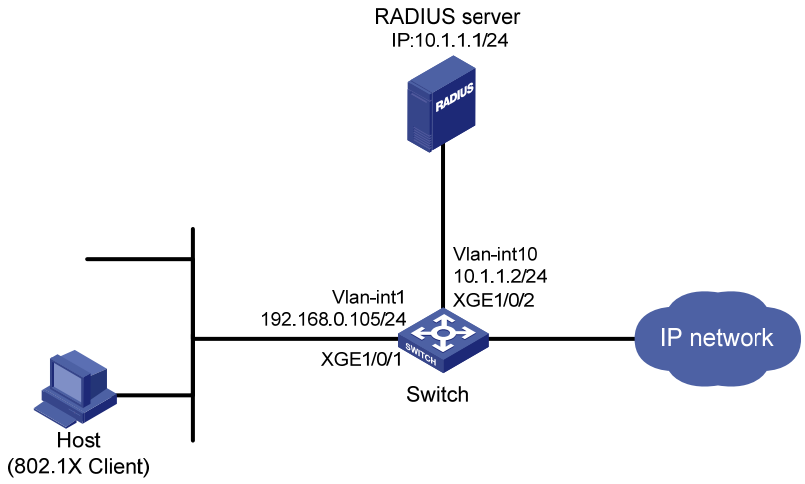
Network requirements

As shown in Figure 8, users must pass 802.1X authentication to access the network. They use HP iNode client on the host to initiate 802.1X authentication.

The switch uses the RADIUS server to perform 802.1X authentication. The RADIUS server runs on IMC.

Configure Ten-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 runs on IMC PLAT 5.2 (E0401) and IMC UAM 5.2 (E0402). The configuration user interface varies with IMC versions, deployed service components, and UAM system settings. For more information, see *HP IMC User Access Manager Administrator Guide*.

Configuration procedures

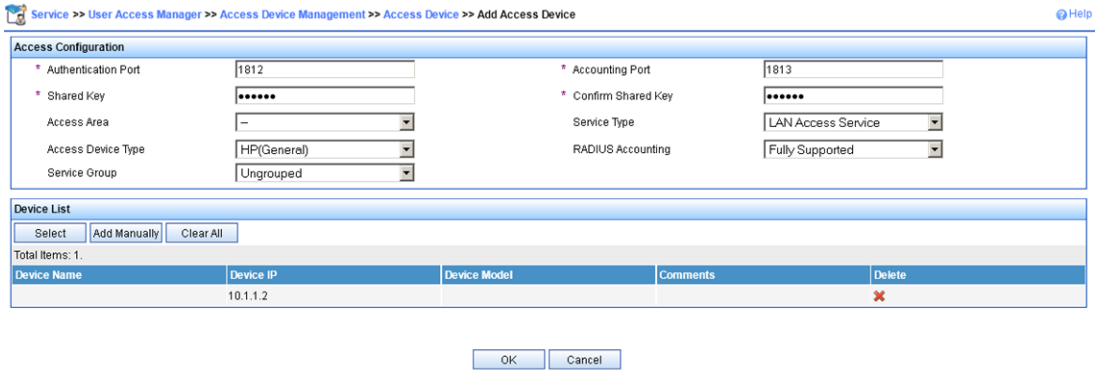
Configuring IP addresses

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

Configuring the RADIUS server

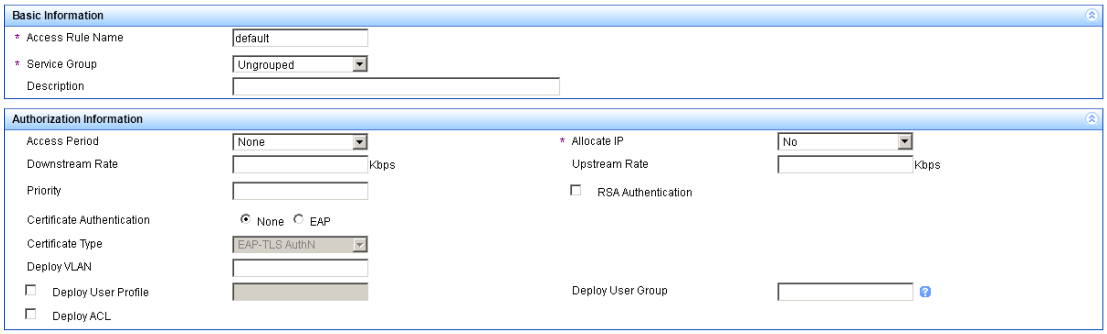
1. Add the switch to IMC as an access device:
   a. Click the **Service** tab.
   b. From the navigation tree, select **User Access Manager** > **Access Device Management** > **Access Device**.
   c. Click **Add**.
   d. In the **Access Configuration** area, specify the following parameters:
      – 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



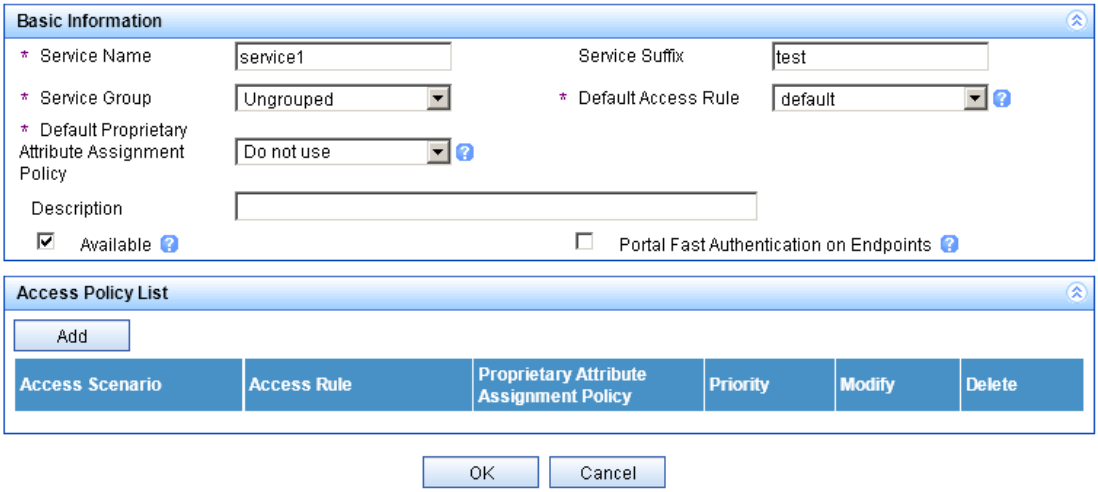
2. Add an access rule:
   a. Click the **Service** tab.
   b. From the navigation tree, select **User Access Manager** > **Access Rule Management**.
   c. Click **Add**.
   d. Enter **default** in the **Access Rule Name** field, and use the default settings for other parameters.
   e. Click **OK**.

Figure 10 Adding an access rule in IMC



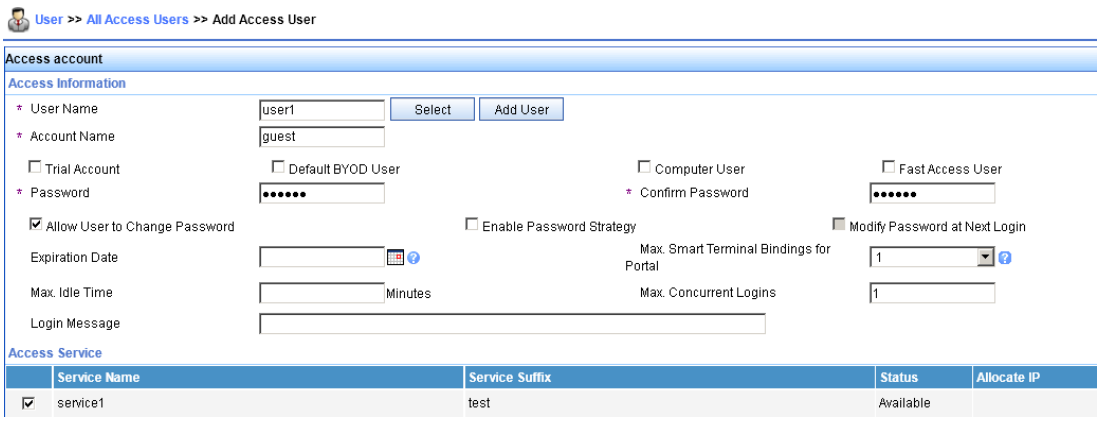
3. Add a service:
   a. Click the **Service** tab.
   b. From the navigation tree, select **User Access Manager** > **Service Configuration**.
   c. Click **Add**.
   d. In the **Basic Information** area, specify the following parameters:
      – Enter **service1** in the **Service Name** field.
      – 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. From the navigation tree, select **Access User View** > **All Access Users**.
   c. Click **Add**.
   d. In the **Access Information** area, click **Add User** to create a Platform user named **user1**.
   e. Configure the user account:
      – 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
```

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** in plain text.

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

Set the response timeout time of the RADIUS server to 5 seconds.

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

Set the maximum number of RADIUS packet retransmission attempts to five.

```
[Switch-radius-radius1] retry 5
[Switch-radius-radius1] quit
```

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

```
[Switch] domain test
```

Configure ISP domain **test** to use RADIUS scheme **radius1** for authentication and authorization of all LAN 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
```

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

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

Configure port Ten-GigabitEthernet 1/0/1 to implement MAC-based access control. By default, the port implements MAC-based access control.

```
[Switch-Ten-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-Ten-GigabitEthernet1/0/1] quit
```

Enable 802.1X globally.

```
[Switch] dot1x
```

Configuring the 802.1X client

Configure the iNode client in the same way the iNode client is configured in "Example: Configuring RADIUS-based 802.1X authentication (non-IMC server)."

Verifying the configuration

Verify that you can use the user account to pass 802.1X authentication:

Double-click **My 802.1X Connection** on the iNode client.

On the **My 802.1X Connection** window, enter username **guest@test** and password **123456**.

Click **Connect**.

Configuration files

```
#
 domain default enable test
#
 dot1x
```

```
#
vlan 1
#
radius scheme radius1
 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
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/1
 dot1x
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 10
#
```

Example: Configuring 802.1X unicast trigger

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

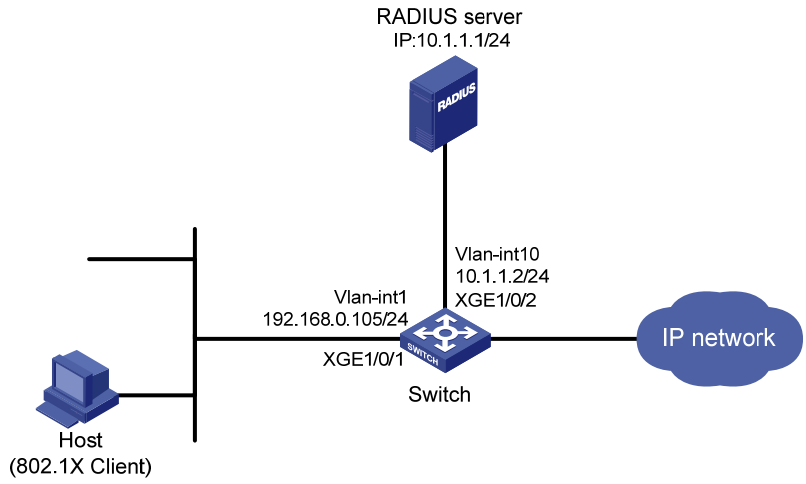
Network requirements

As shown in Figure 13, users must pass 802.1X authentication to access the network. They use the built-in 802.1X client of Windows XP on the host, which cannot initiate 802.1X authentication.

Configure the switch to perform the following operations:

- Initiate 802.1X authentication.
- Use the RADIUS server to provide authentication and authorization services for the 802.1X users. IMC runs on the server.
- Implement MAC-based access control on GigabitEthernet 1/0/1. Each user is separately authenticated. When a user logs off, no other online users are affected.

Figure 13 Network diagram



Requirements analysis

For the switch to initiate 802.1X authentication, you must enable an authentication trigger function on the switch.

To ensure system performance, HP recommends that you disable the 802.1X multicast trigger function and enable the unicast trigger function. In multicast trigger mode, the switch multicasts a large number of Identity EAP-Request packets periodically to the host, which consumes bandwidth and system resources.

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

Configure the RADIUS server in the same way the RADIUS server is configured in "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
```

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** in plain text.

```
[Switch-radius-radius1] key authentication simple aabbcc
[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** for authentication and authorization of all LAN 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
```

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

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

Enable the 802.1X unicast trigger function on the port.

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

Enable 802.1X on the port.

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

Configure the port to implement MAC-based access control. By default, the port implements MAC-based access control.

```
[Switch-Ten-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-Ten-GigabitEthernet1/0/1] quit
```

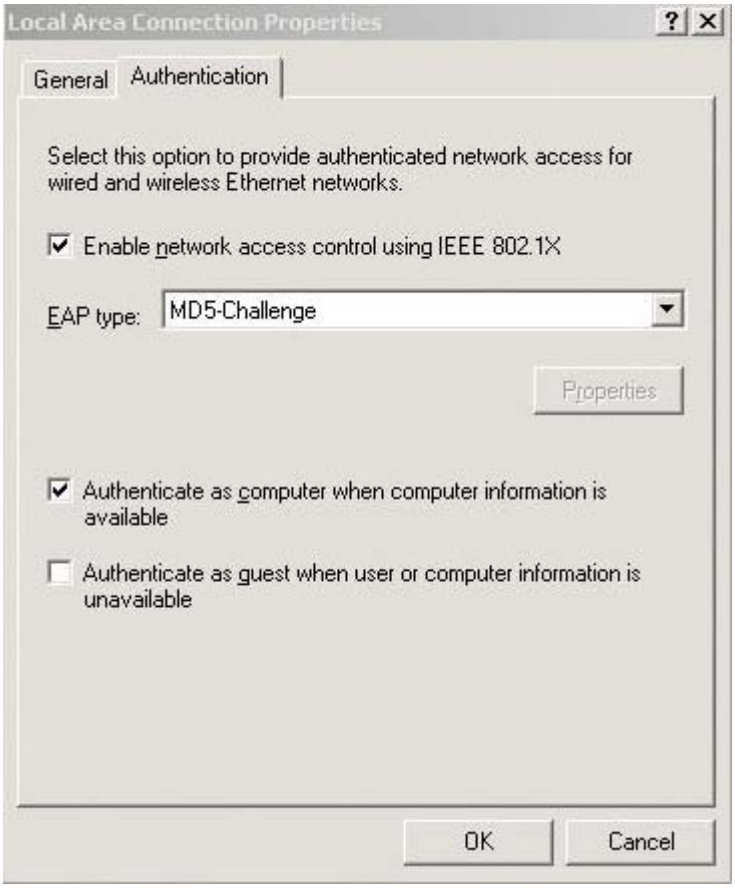
Enable 802.1X globally.

```
[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

Verify that you can use the user account to pass 802.1X authentication:

Use the host to visit an Internet Webpage. The Windows status bar displays a message and asks you to enter your username and password.

Enter username **guest@test** and password **123456**.

Configuration files

```
#
 domain default enable test
#
 dot1x
#
radius scheme radius1
 primary authentication 10.1.1.1
 key authentication $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication default radius-scheme radius1
```

```
 authorization default radius-scheme radius1
#
interface Ten-GigabitEthernet1/0/1
 undo dot1x multicast-trigger
 dot1x
 dot1x unicast-trigger
```

AAA configuration examples

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

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. Terminal users can access through a console port.

Example: Configuring local authentication and authorization for FTP users

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

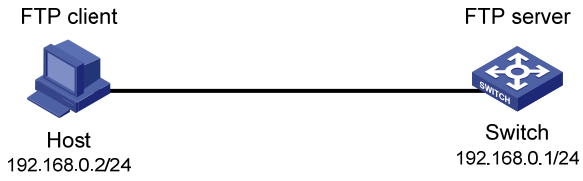
Network requirements

As shown in Figure 15, users on the host can access the switch through FTP. The FTP username is **ftpuser** and password is **aabbcc**.

Configure the switch to meet the following requirements:

- Implement local authentication and authorization for FTP users.
- Remove the default user role from the FTP users and assign user role **network-admin** after FTP users pass authentication.

Figure 15 Network diagram



Requirements analysis

To make the switch implement local authentication and authorization, you must specify the **local** method for authentication and authorization in the ISP domain where the FTP users are authenticated.

Configuration restrictions and guidelines

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

- The device supports up to 16 ISP domains, including the system-defined ISP domain **system**. You can specify one of the ISP domains as the default domain.
- On the device, each user belongs to an ISP domain. If a user does not have an ISP domain name, the device assigns the default ISP domain to the user. By default, the default ISP domain is **system**.
- To delete the ISP domain functioning as the default ISP domain, change the domain to a non-default ISP domain by using the **undo domain default enable** command.
- To log in to the device, a user must obtain at least one user role from the AAA server or the local device. You can enable the default user role function or assign a user role to the user.

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
```

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

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

Create a device management user **ftpuser**.

```
[Switch] local-user ftpuser class manage
```

Set the password to **aabbcc** in plain text for the user.

```
[Switch-luser-manage-ftpuser] password simple aabbcc
```

Authorize the FTP service to the user.

```
[Switch-luser-manage-ftpuser] service-type ftp
```

Assign user role **network-admin** to the user.

```
[Switch-luser-manage-ftpuser] authorization-attribute user-role network-admin
```

Remove the default user role of the user.

```
[Switch-luser-manage-ftpuser] undo authorization-attribute user-role network-operator
[Switch-luser-manage-ftpuser] quit
```

Verifying the configuration

Access the switch through FTP by using username **ftpuser** and password **aabbcc**. 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)):ftpuser
331 Password required for ftpuser.
Password:
230 User logged in.
ftp>
```

Display configuration and statistics for user **ftpuser**.

```
[Switch] display local-user user-name ftpuser class manage
Total 1 local users matched.

Device management user ftpuser:
 State:                    Active
 Service Type:             FTP
 User Group:               system
 Bind Attributes:
 Authorization Attributes:
  Work Directory:          flash:
  User Role List:          network-admin
```

The output shows that the FTP user is assigned the user role **network-admin**.

Configuration files

```
#
 ftp server enable
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.1 255.255.255.0
#
domain system
 authentication login local
 authorization login local
#
 domain default enable system
#
local-user ftpuser class manage
 password hash $h$6$4TEfp9hT6mqaVPHI$0nEZB12248SABi3eD7Zs+wsvicOCzJR24tt5li0og7E
jmmwHpS/Flt+38hqtYSxxw27IG4Y7bg8JHZhpuTN40A==
 service-type ftp
 authorization-attribute user-role network-admin
#
```

Example: Configuring RADIUS authentication and authorization for SSH users

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

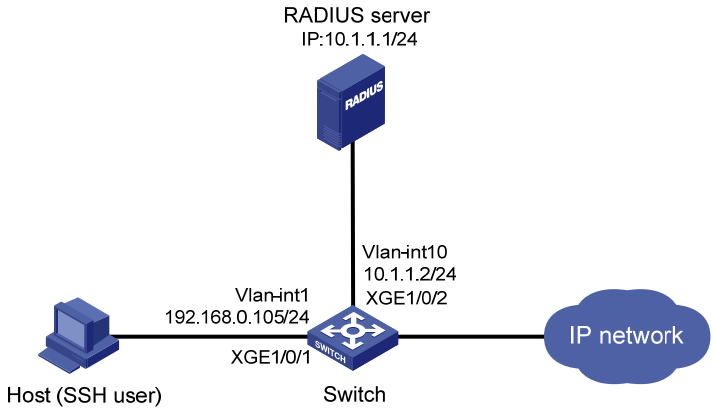
As shown in Figure 16, the RADIUS authentication and authorization server runs on IMC.

Configure the switch to meet the following requirements:

- Use the RADIUS server for SSH user authentication and authorization.
- Assign the default user role **network-operator** to SSH users after they pass authentication.
- Send usernames with domain names to the RADIUS server.
- Use **aabbcc** as the shared keys for secure RADIUS communication.

Add an account with the username **hello@bbb** and password **123456** on the RADIUS server. SSH users log in to the switch by using this account.

Figure 16 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To implement remote RADIUS authentication and authorization, you must 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 authorization information.

- To communicate with the RADIUS server and host, you must configure the switch as the RADIUS client and SSH server.
- To make the switch assign the default user role **network-operator** to SSH users, you must enable the default user role function on the switch.

Configuration restrictions and guidelines

The RADIUS server runs on IMC PLAT 5.2 (E0401) and IMC UAM 5.2 (E0402). The configuration user interface varies depending on the IMC versions, deployed service components, and UAM system settings. For more information, see *IMC User Access Manager Administrator Guide*.

Configuration procedures

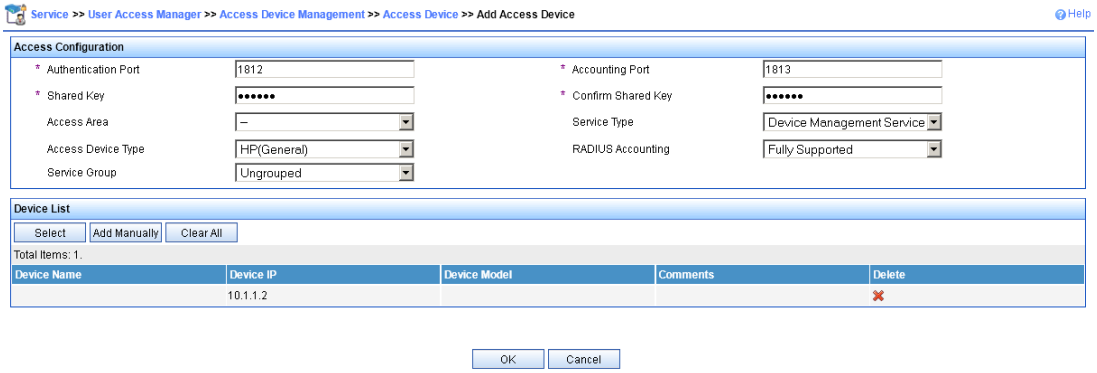
Configuring interfaces

Configure the IP addresses for interfaces as shown in Figure 16, 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. From the navigation tree, select **User Access Manager** > **Access Device Management** > **Access Device**.
   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 **Device Management 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 access device IP address.
   f. Click **OK**.

Figure 17 Adding an access device in IMC



2. Create a device management user account for the SSH user:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Manager** > **Access User View** > **Device Mgmt User**.
   c. Click **Add**.
   d. 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.
      – Enter **network-operator** in the **Role Name** field.
   e. In the **IP Address List of Managed Devices** area, click **Add** to specify 10.1.1.2 as the start and end IP addresses.
   f. Click **OK**.

Figure 18 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 ten-gigabitethernet 1/0/2
[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 key pair.

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

Create a local DSA key pair.

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+.............+.............+...+.....+.............+..+...
...+.................+..........+...+....+.......+.....+............+.........+.
.........................+........+..........+.............+.....+...+..........
..............+.........+..........+...........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Enable the SSH server function.

```
[Switch] ssh server enable
```

Enable **scheme** authentication on user interfaces VTY 0 through VTY 15.

```
[Switch] user-interface vty 0 15
```

```
[Switch-ui-vty0-15] authentication-mode scheme
```

Enable user interfaces VTY 0 through VTY 15 to support only SSH.

```
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
```

Enable the default user role function. The authenticated SSH users are assigned the default user role **network-operator**.

```
[Switch] role default-role enable
```

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** in plain text.

```
[Switch-radius-rad] key authentication simple 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
[Switch-radius-rad] quit
```

Create ISP domain **bbb**.

```
[Switch] domain bbb
```

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

```
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit
```

Configuring the host

Configure the SSH client on the host. The configuration procedure varies by SSH client software. (Details not shown.)

For more information, see *SSH Configuration Examples*.

Verifying the configuration

Initiate an SSH connection to the switch, and enter the username **hello@bbb** and password **123456**. The user logs in to the switch. (Details not shown.)

Verify that the user can use the commands permitted by the **network-operator** user role. (Details not shown.)

Configuration files

```
#
vlan 10
#
interface Vlan-interface10
```

```
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 10
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
 protocol inbound ssh
#
 ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 key authentication cipher $c$3$S7yuRSTuxsoBlCzxhXVUbzci7XRMRNGAHA==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login none
#
```

Example: Configuring LDAP authentication for SSH users

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

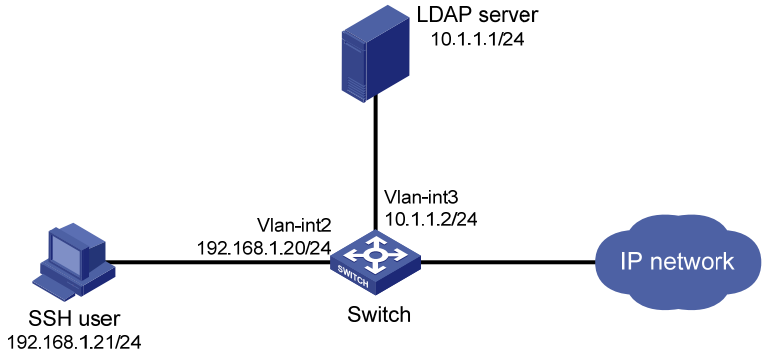
As shown in Figure 19, an LDAP server is located at 10.1.1.1/24 and uses the domain name **ldap.com**.

Configure the switch to meet the following requirements:

- Use the LDAP server to authenticate SSH users.
- Assign the default user role **network-operator** to SSH users after they pass authentication.

On the LDAP server, set the administrator password to **admin!123456**, add user **aaa**, and set the user's password to **ldap!123456**.

Figure 19 Network diagram



Configuration restrictions and guidelines

When you configure LDAP authentication, follow these restrictions and guidelines:

- The device supports LDAPv2 and LDAPv3. The LDAP version specified on the device must be consistent with the version specified on the LDAP server.
- The device does not support LDAP authorization.

Configuration procedure

1. Configure the LDAP server:

NOTE:

In this example, the LDAP server runs Microsoft Windows 2003 Server Active Directory.

Add a user named **aaa** and set the password to **ldap!123456**.

a. On the LDAP server, select **Start** > **Control Panel** > **Administrative Tools**.

b. Double-click **Active Directory Users and Computers**.

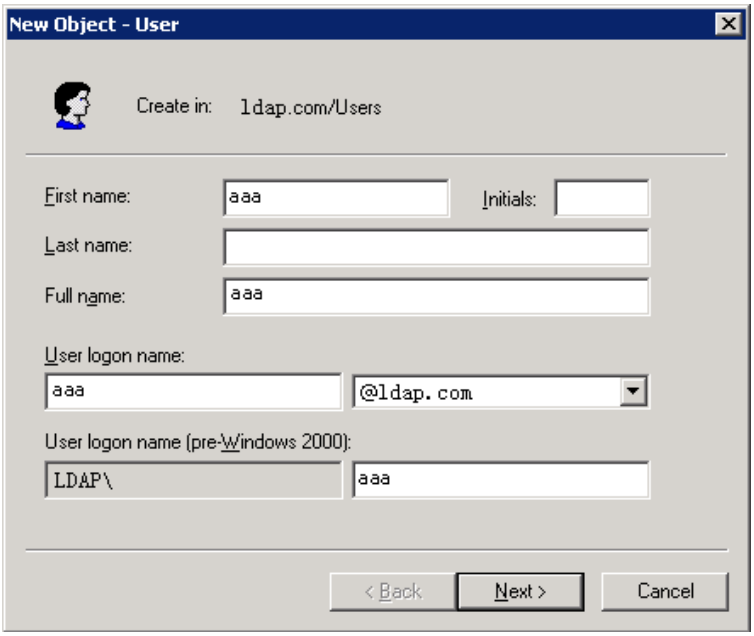
The **Active Directory Users and Computers** window is displayed.

c. From the navigation tree, click **Users** under the **ldap.com** node.

d. Select **Action** > **New** > **User** from the menu to display the dialog box for adding a user.

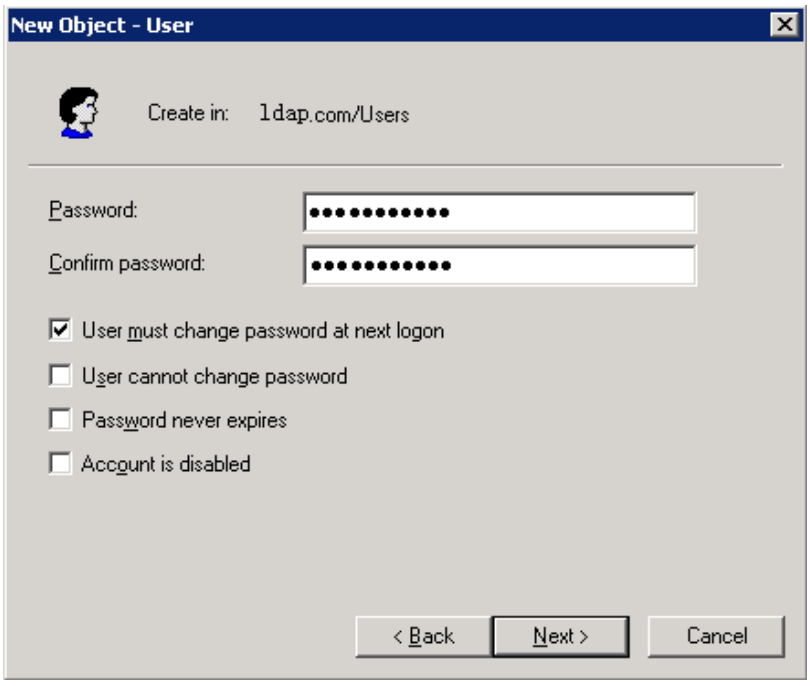
e. Enter the login name **aaa** and click **Next**.

Figure 20 Adding user aaa



f. In the dialog box, enter the password **ldap!123456**, select options as needed, and click **Next**.

Figure 21 Setting the user's password



g. Click **OK**.

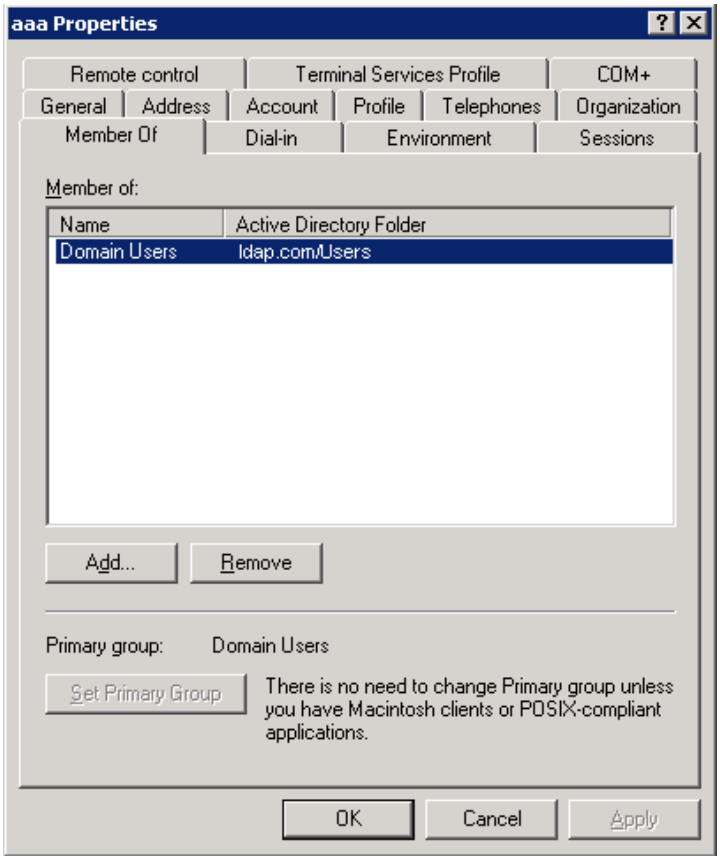
Add user **aaa** to group **Users**.

a. From the navigation tree, click **Users** under the **ldap.com** node.

b. On the right pane, right-click **aaa** and select **Properties**.

c. In the dialog box, click the **Member Of** tab and click **Add**.

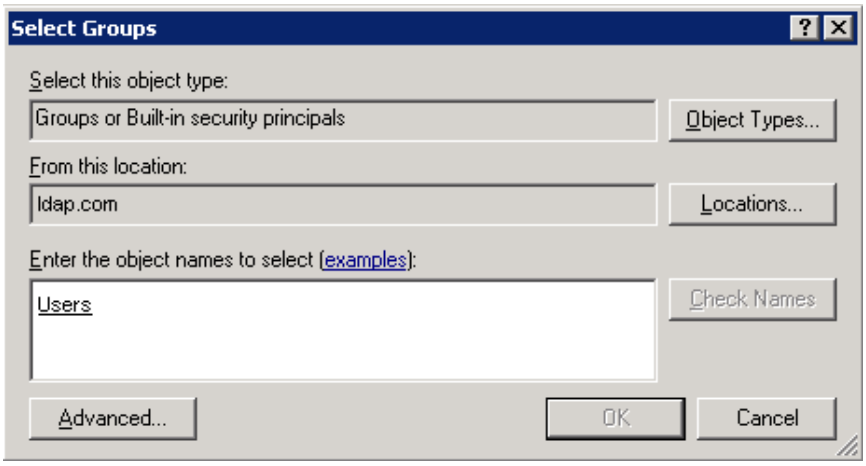
Figure 22 Modifying user properties



d. In the **Select Groups** dialog box, enter **Users** in the **Enter the object names to select** field, and click **OK**.

User **aaa** is added to group **Users**.

Figure 23 Adding user aaa to group Users



Set the administrator password to **admin!123456**.

a. From the user list on the right pane, right-click **Administrator** and select **Set Password**.

b. In the dialog box, enter the administrator password. (Details not shown.)

2. Configure the switch:

Assign an IP address to VLAN-interface 2, the SSH user access interface.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.20 24
[Switch-Vlan-interface2] quit
```

Assign an IP address to VLAN-interface 3, through which the switch communicates with the LDAP server.

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 24
[Switch-Vlan-interface3] quit
```

Create a local RSA key pair.

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

Create a local DSA key pair.

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+.........+............+............+...+.....+............+..+...
...+.................+.........+...+....+.......+.....+...........+.........+.
.........................+........+.........+.............+.....+...+.........
.............+.........+.........+..........+........+....+.................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Enable the SSH server function.

```
[Switch] ssh server enable
```

Enable **scheme** authentication on user interfaces VTY 0 through VTY 15.

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

Enable the default user role function. The authenticated SSH users are assigned the default user role **network-operator**.

```
[Switch] role default-role enable
```

Configure an LDAP server.

```
[Switch] ldap server ldap1
```

Specify the IP address of the LDAP authentication server.

```
[Switch-ldap-server-ldap1] ip 10.1.1.1
```

Specify the administrator DN.

```
[Switch-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ldap,dc=com
```

Specify the administrator password.

```
[Switch-ldap-server-ldap1] login-password simple admin!123456
```

Configure the base DN for user search.

```
[Switch-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[Switch-ldap-server-ldap1] quit
```

Create an LDAP scheme.

```
[Switch] ldap scheme ldap-shm1
```

Specify the LDAP authentication server.

```
[Switch-ldap-ldap-shm1] authentication-server ldap1
[Switch-ldap-ldap-shm1] quit
```

Create ISP domain **bbb**.

```
[Switch] domain bbb
```

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

```
[Switch-isp-bbb] authentication login ldap-scheme ldap-shm1
[Switch-isp-bbb] authorization login none
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit
```

Verifying the configuration

Initiate an SSH connection to the switch, and enter the username **aaa@bbb** and password **ldap!123456**. The user logs in to the switch. (Details not shown.)

Verify that the user can use the commands permitted by the **network-operator** user role. (Details not shown.)

Configuration files

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.20 255.255.255.0
#
vlan 3
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
```

```
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
#
ldap server ldap1
 login-dn cn=administrator,cn=users,dc=ldap,dc=com
 search-base-dn dc=ldap,dc=com
 ip 10.1.1.1
 login-password cipher $c$3$2yaMeNBO6mF7267n61Bow4cNHoMhBAT2muA6wyHp2A==
#
ldap scheme ldap-shm1
 authentication-server ldap1
#
domain bbb
 authentication login ldap-scheme ldap-shm1
 authorization login none
 accounting login none
#
```

ACL configuration examples

This chapter provides ACL configuration examples.

NOTE:

The **config** match order is used in the ACL examples. For information about ACL match orders, see *HP 5920 & 5900 Switch Series ACL and QoS Configuration Guide*.

Example: Allowing a specific host to access the network

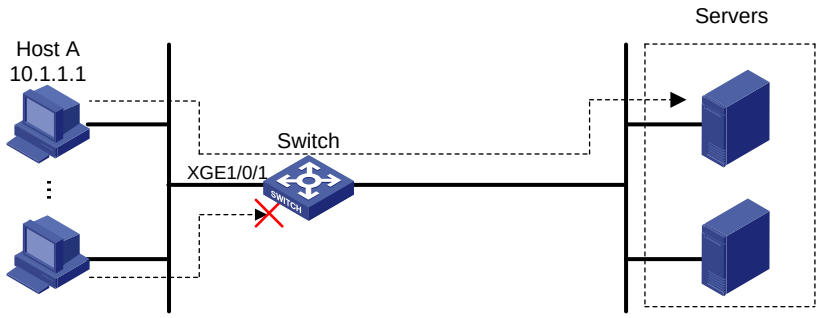
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 24, apply an ACL to Ten-GigabitEthernet 1/0/1 to allow packets sourced from Host A only during working hours (from 8:30 to 18:00) every day.

Figure 24 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To implement time-based ACL rules, 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, configure a deny statement after the permit statement.

Configuration restrictions and guidelines

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

- The wildcard mask is used with an IP address to define a subnet in an ACL rule. 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**.
- Configure the permit statement before the deny statement. Otherwise, the interface denies all packets to pass through during working hours.

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 permit packets sourced from 10.1.1.1 during working hours.

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

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

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 2000
```

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

Ping a server from Host A during working hours. The server can be pinged successfully. Ping a server from a host other than Host A. The server cannot be pinged. (Details not shown.)

During a period other than the working hours, ping a server from any host. The server can be pinged successfully. (Details not shown.)

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
```

```
#
interface Ten-GigabitEthernet1/0/1
 packet-filter 2000 inbound
#
```

Example: Denying a specific host to access the network

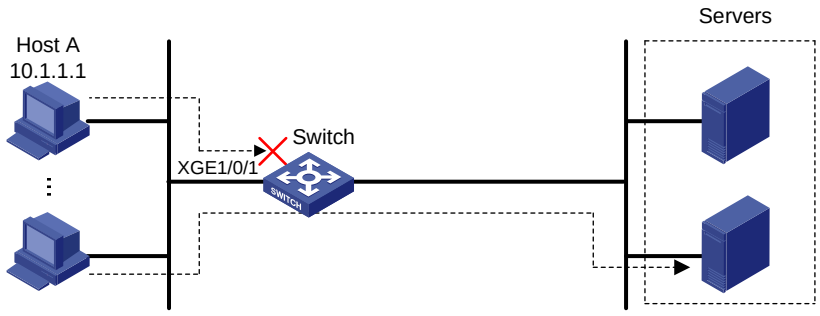
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 25, apply an ACL to Ten-GigabitEthernet 1/0/1 to deny packets sourced from Host A only during working hours (from 8:30 to 18:00) every day.

Figure 25 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:

- The wildcard mask is used with an IP address to define a subnet in an ACL rule. 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 during working hours.

```
[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 Ten-GigabitEthernet1/0/1.

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 2000
```

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

Ping a server from Host A during working hours. The server cannot be pinged. Ping a server from a host other than Host A. The server can be pinged successfully. (Details not shown.)

During a period other than the working hours, ping a server from any host. The server can be pinged successfully. (Details not shown.)

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 Ten-GigabitEthernet1/0/1
 packet-filter 2000 inbound
#
```

Example: Allowing access between specific subnets

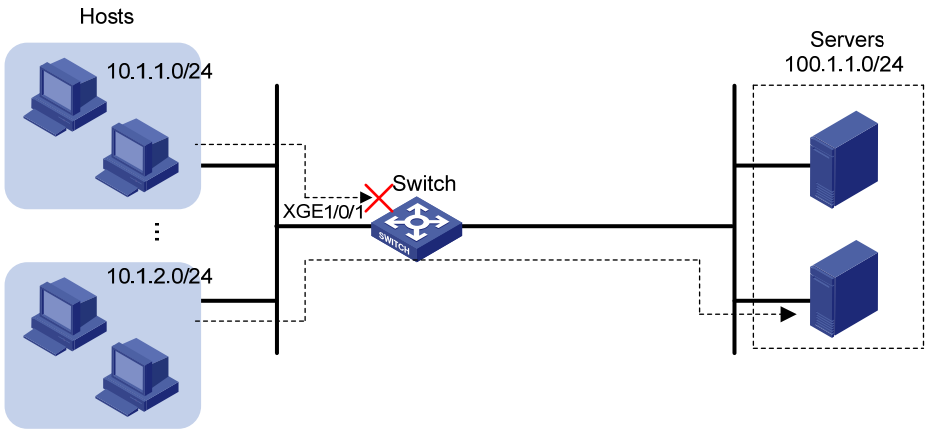
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 26, apply an ACL to Ten-GigabitEthernet 1/0/1 to allow only packets from 10.1.2.0/24 to 100.1.1.0/24.

Figure 26 Network diagram



Configuration restrictions and guidelines

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

- The wildcard mask is used with an IP address to define a subnet in an ACL rule. 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**.
- Configure the permit statement before the deny statement. Otherwise, the interface denies all packets to pass through.

Configuration procedures

Create IPv4 advanced ACL 3000. Configure two rules in the ACL. One permits IP packets from 10.1.2.0/24 to 100.1.1.0/24, and the other denies IP packets to pass through.

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

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

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

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 3000
```

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

Ping a server on subnet 100.1.1.0/24 from a host on subnet 10.1.2.0/24. The server can be pinged successfully. (Details not shown.)

Ping a server on subnet 100.1.1.0/24 from a host on another subnet. The server cannot be pinged. (Details not shown.)

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 Ten-GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
```

Example: Denying Telnet packets

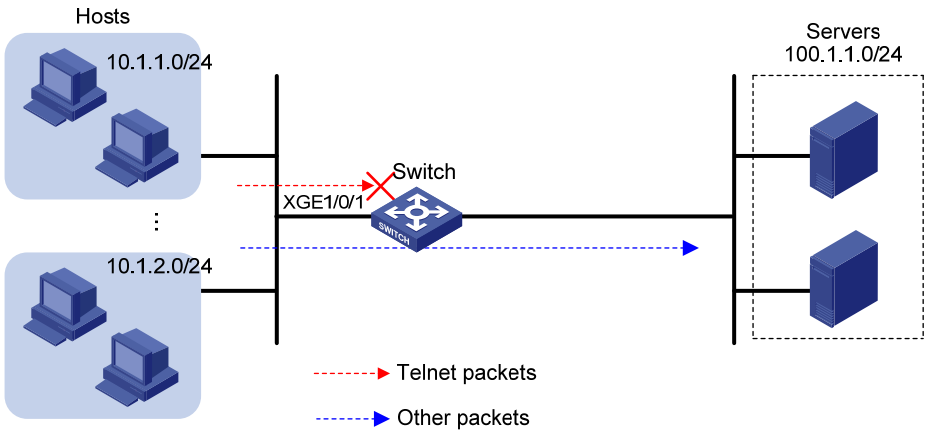
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 27, apply an ACL to Ten-GigabitEthernet 1/0/1 to deny all incoming Telnet packets and permit other IP packets.

Figure 27 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 Ten-GigabitEthernet 1/0/1.

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 3000
```

The output shows that ACL 3000 has been applied successfully to Ten-GigabitEthernet 1/0/1 for incoming 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. The Telnet operation fails. (Details not shown.)

Configuration files

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

Example: Allowing TCP connections initiated from a specific subnet

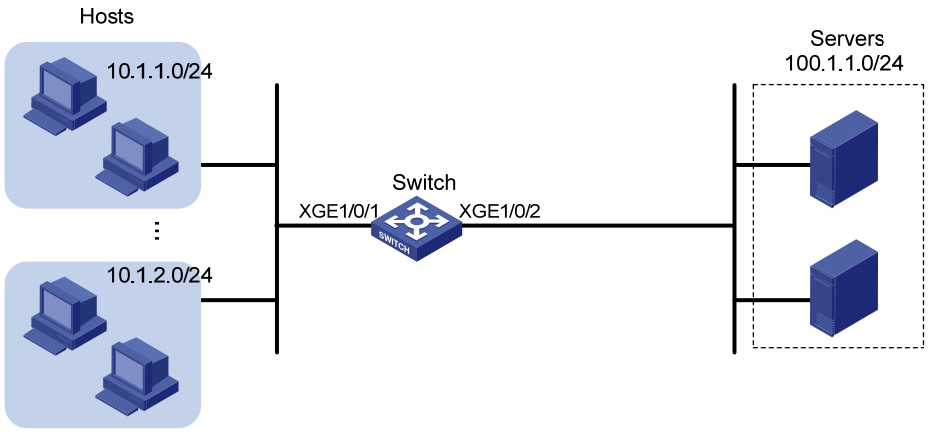
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 28, apply an ACL to allow TCP connections between the hosts and servers except those initiated by the servers to hosts on subnet 10.1.1.0/24.

Figure 28 Network diagram



Requirements analysis

To allow TCP connections except those initiated by the servers to hosts on subnet 10.1.1.0/24, you must perform the following tasks:

- Specify the **established** keyword (the ACK or RST flag bit set) in the advanced ACL rule to match established TCP connections.
- Because a TCP initiator typically uses a TCP port number greater than 1023, specify a port number range greater than 1023 to match established TCP connections.

Configuration restrictions and guidelines

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

- The wildcard mask is used with an IP address to define a subnet in an ACL rule. 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**.
- Configure the permit statement before the deny statement. Otherwise, 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 on 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 connections initiated by the servers to the hosts on 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 Ten-GigabitEthernet 1/0/2.

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/2.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/2
Interface: Ten-GigabitEthernet1/0/2
  In-bound Policy:
    ACL 3000
```

The output shows that ACL 3000 has been applied successfully to Ten-GigabitEthernet 1/0/2 for incoming 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. (Details not shown.)

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. (Details not shown.)

Verify that hosts on subnet 10.1.2.0/24 and servers can access shared folders of each other. (Details not shown.)

Configuration files

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

Example: Denying FTP traffic

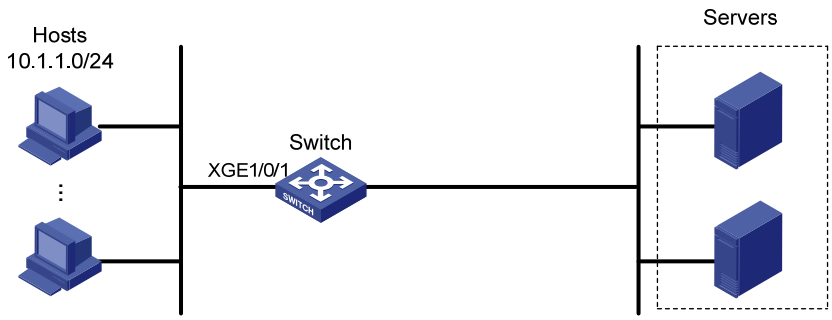
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 29, apply an ACL to Ten-GigabitEthernet 1/0/1 to deny FTP traffic destined for the servers.

Figure 29 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 configure 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 Ten-GigabitEthernet 1/0/1.

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 3000
```

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

Use a host to initiate FTP connection requests to a server that provides FTP services. FTP connection cannot be established. (Details not shown.)

Configuration files

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

Example: Allowing FTP traffic (active FTP)

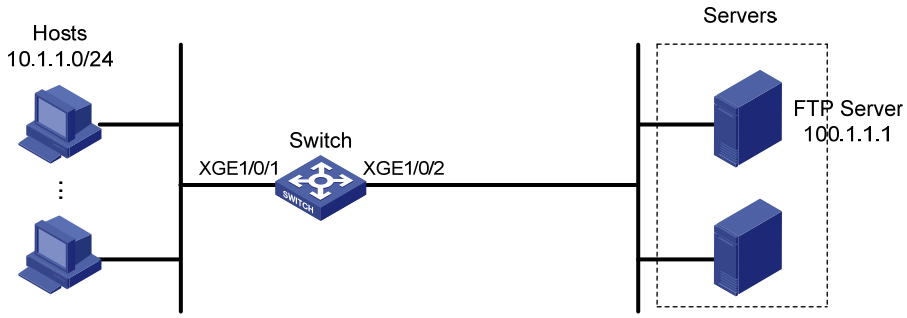
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 30, apply an ACL to permit active FTP traffic and deny all other IP traffic.

Figure 30 Network diagram



Requirements analysis

FTP active mode uses two connections between the client and the server:

- The client initiates the control connection from client port 20 to the server port 21.
- The server initiates the data connection from port 20 to the client specified random port.

To meet the network requirements, you must perform the following tasks:

- To match FTP control protocol packets, specify TCP port 21 in a rule.
- To match established FTP data connections, 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 Ten-GigabitEthernet 1/0/1.

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

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

Verifying the configuration

Use the **display packet-filter interface** command to display ACL application information for packet filtering on all interfaces.

```
[Switch] display packet-filter interface
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 3000
  Interface: Ten-GigabitEthernet1/0/2
  In-bound Policy:
    ACL 3001
```

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

Verify that you can obtain data from a server through FTP when the server operates in active FTP mode. (Details not shown.)

Verify that you cannot obtain data from a server through FTP when the server operates in passive FTP mode. (Details not shown.)

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 eq ftp-data established
 rule 10 deny ip
acl number 3001
 rule 0 permit tcp source 100.1.1.1 0 source-port eq ftp-data established
 rule 5 permit tcp source 100.1.1.1 0 source-port eq ftp
 rule 10 deny ip
#
interface Ten-GigabitEthernet1/0/1
 packet-filter 3000 inbound
#
interface Ten-GigabitEthernet1/0/2
 packet-filter 3001 inbound
```

Example: Allowing FTP traffic (passive FTP)

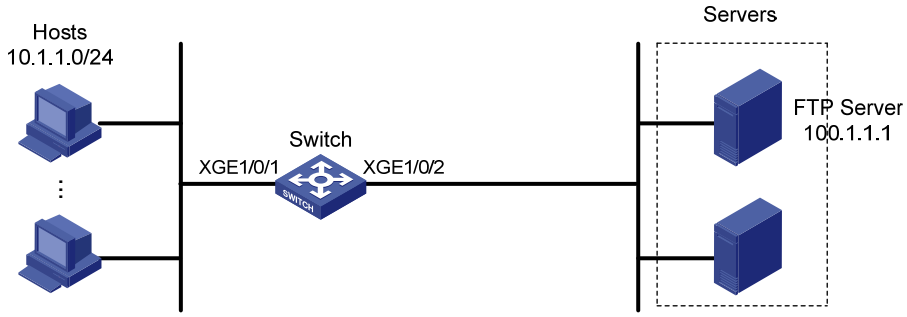
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 31, apply an ACL to permit only passive FTP traffic and deny all other IP traffic.

Figure 31 Network diagram



Requirements analysis

In FTP passive 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. To meet the network requirements, you must perform the following tasks:

- To match FTP protocol control packets destined for the FTP server, specify destination TCP port 21 in a rule.
- To match established FTP data connections destined for the FTP server, specify the **established** keyword and destination TCP port greater than 1024 in a rule.
- To match established FTP protocol control packets destined for the FTP client, specify source TCP port 21 in a rule.
- To match established FTP data connections destined for the FTP client, specify the **established** keyword and source TCP port greater than 1024 in a rule.

Configuration restrictions and guidelines

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

- The wildcard mask is used with an IP address to define a subnet in an ACL rule. 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**.
- Configure the permit statement before the deny statement. Otherwise, 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 Ten-GigabitEthernet 1/0/1.

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

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

Verifying the configuration

Use the **display packet-filter interface** command to display ACL application information for packet filtering on all interfaces.

```
[Switch] display packet-filter interface
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 3000
  Interface: Ten-GigabitEthernet1/0/2
  In-bound Policy:
    ACL 3001
```

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

Verify that you can obtain data from a server through FTP when the server operates in passive FTP mode. (Details not shown.)

Verify that you cannot obtain data from a server through FTP when the server operates in active FTP mode. (Details not shown.)

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

Example: Allowing ICMP requests from a specific direction

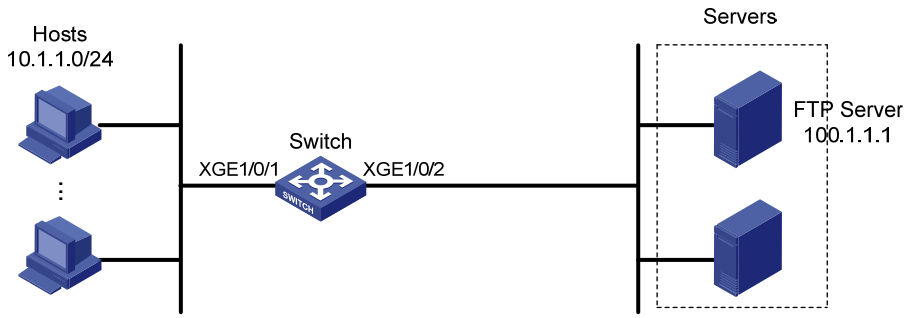
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 32, apply an ACL to deny ICMP requests from the FTP server to the hosts. Only hosts can ping the FTP server.

Figure 32 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 Ten-GigabitEthernet 1/0/2.

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/2.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/2
Interface: Ten-GigabitEthernet1/0/2
  In-bound Policy:
    ACL 3000
```

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

Ping the FTP server from a host. The FTP server can be pinged successfully. (Details not shown.)

Ping the host from the FTP server. The host cannot be pinged. (Details not shown.)

Configuration files

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

Example: Allowing HTTP/email/DNS traffic

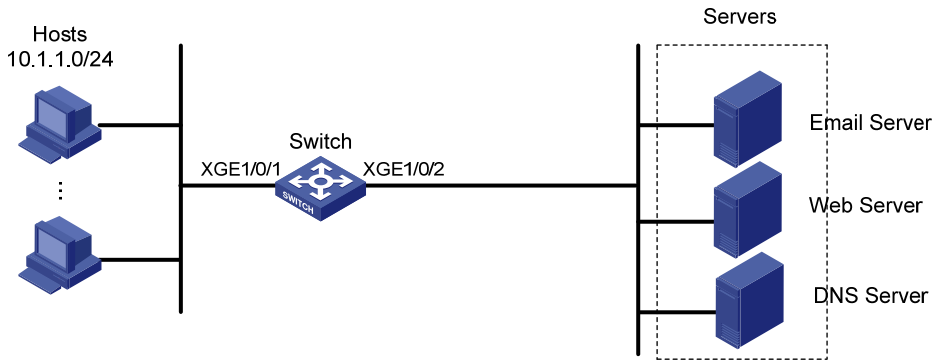
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 33, apply an ACL to Ten-GigabitEthernet 1/0/1 to allow only Email, HTTP, and DNS traffic from the server to the hosts. Other traffic sourced from the servers to the hosts is denied.

Figure 33 Network diagram



Configuration restrictions and guidelines

Configure the permit statement before the deny statement. Otherwise, the interface denies all packets to pass through.

Configuration procedures

Create IPv4 advanced ACL 3000 and configure the rules to permit only packets with destination TCP port 25 (SMTP), 110 (POP3), 80 (HTTP), and 53 (DNS).

```
<Switch> system-view
[Switch] acl number 3000
[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 Ten-GigabitEthernet 1/0/1.

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

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 3000
```

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

Ping a server from a host. The server cannot be pinged. (Details not shown.)

Verify that the hosts can obtain HTTP services from the HTTP server, Email service from the Email server, and DNS service from the DNS server. (Details not shown.)

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 Ten-GigabitEthernet1/0/1
 packet-filter 3000 inbound
```

Example: Filtering packets by MAC address

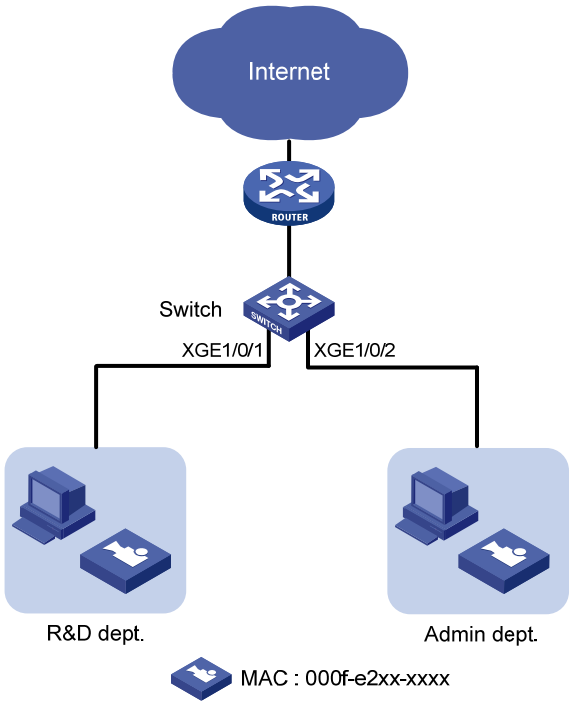
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 34, 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 34 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To match packets from or to a device whose IP address might change, use Layer 2 ACLs. Layer 2 ACLs (4000 to 4999) match packets based on Layer 2 protocol header fields, such as source and destination MAC addresses, 802.1p priority, and link layer protocol type.
- To specify devices with the same MAC address prefix, 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 time2 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] packet-filter 4000 inbound
[Switch-Ten-GigabitEthernet1/0/1] quit
[Switch] interface ten-gigabitethernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] packet-filter 4000 inbound
```

Verifying the configuration

Use the **display packet-filter** command to display ACL application information for packet filtering on Ten-GigabitEthernet 1/0/1.

```
[Switch] display packet-filter interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
  In-bound Policy:
    ACL 4000
```

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

Verify that video devices can communicate with devices in the external network only during the working hours. (Details not shown.)

Configuration files

```
#
 time-range time1 00:00 to 08:30 daily
 time-range time2 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 Ten-GigabitEthernet1/0/1
 packet-filter 4000 inbound
```

Example: Applying ACLs in device management

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

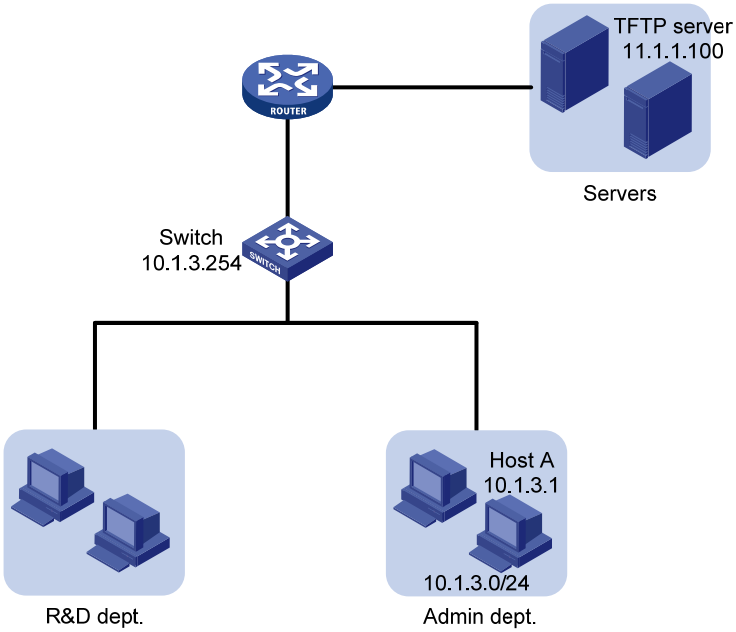
Network requirements

As shown in Figure 35, 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 35 Network diagram



Requirements analysis

To control access to Telnet, FTP, and TFTP, you must configure a basic ACL for each function to permit traffic only sourced from a specific device and apply the ACL to each function.

Configuration restrictions and guidelines

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

- The wildcard mask is used with an IP address to define a subnet in an ACL rule. 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 allow only Host A to Telnet to the switch.

```
[Switch] telnet server acl 2000
```

- 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. (Details not shown.)

Configuration files

```
#
 ftp server enable
 ftp server acl 2002
#
 telnet server acl 2000
#
 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
```

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 blackhole routing

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

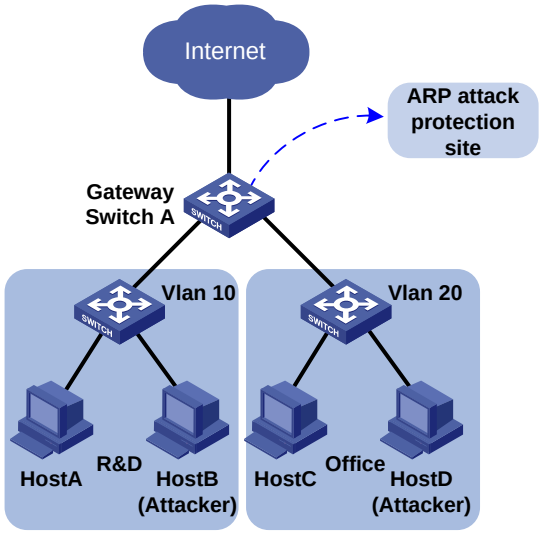
As shown in Figure 36:

- Host B sends a large number of unresolvable IP packets with the same source address.
- Host D sends a large number of unresolvable IP packets with different source addresses.

Configure ARP source suppression and ARP blackhole 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 36 Network diagram



Configuration procedures

1. Configure 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 blackhole 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
```

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.

Configuration files

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

Example: Configuring source MAC-based ARP attack detection

Applicable product matrix

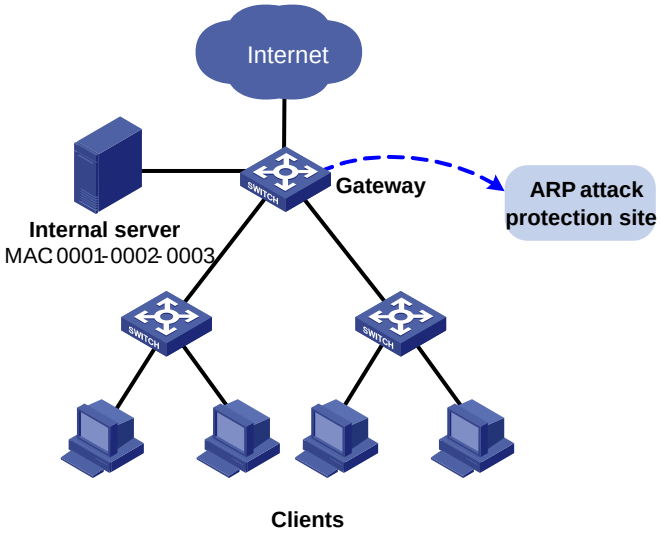
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 37, 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 37 Network diagram



Configuration procedures

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

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

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

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

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

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

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

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

Verifying the configuration

Display source MAC-based ARP attack detection entries.

```
<Sysname> display arp source-mac slot 1
Source-MAC          VLAN ID          Interface              Aging-time
23f3-1122-3344      4094             XGE2/0/1               10
23f3-1122-3355      4094             XGE2/0/2               30
```

```
23f3-1122-33ff      4094            XGE2/0/3            25
23f3-1122-33ad      4094            XGE2/0/4            30
23f3-1122-33ce      4094            XGE2/0/5            2
```

Configuration files

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

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

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

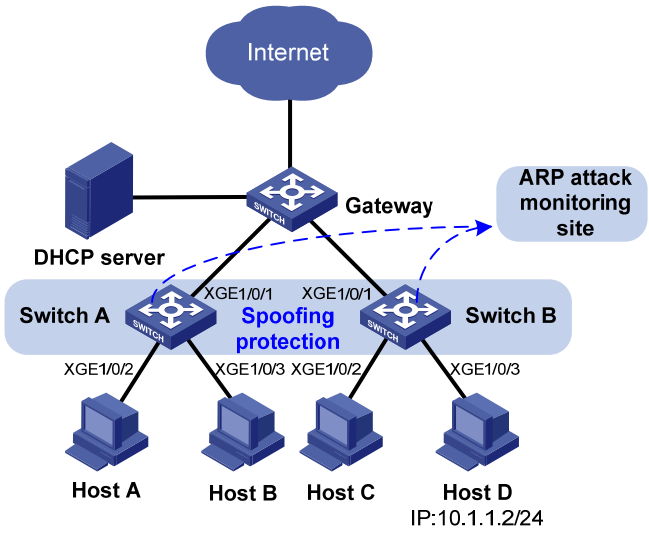
Network requirements

As shown in Figure 38:

- 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. This feature also discards the packets from Host D.

Figure 38 Network diagram



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 enable
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] dhcp snooping trust
   [SwitchA-Ten-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 ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] arp detection trust
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Enable ARP packet validity check.

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

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

Verifying the configuration

Ping the gateway from Host A, Host B, and Host C. All the ping operations succeed.

Ping the gateway from Host D. The ping operation fails.

Configuration files

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

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

Applicable product matrix

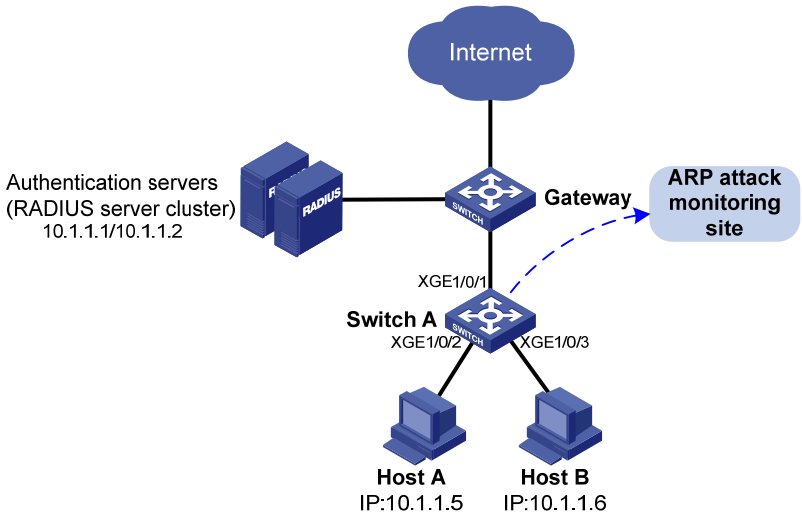
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 39, Host A and Host B use static IP addresses, and they access the gateway and authentication servers through Switch A.

- Configure the following servers:
  - 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 39 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

Add a network access user named **localuser**, and set the password to **localpass** in plain text.

```
<SwitchA> system-view
[SwitchA] local-user localuser class network
[SwitchA-luser-network-localuser] password simple localpass
```

Authorize the network access user **localuser** to use the LAN access service.

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

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 simple name
```

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

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

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

```
[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
```

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
[SwitchA-isp-aabbcc.net] quit
```

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

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

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

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

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. By default, an interface is an untrusted interface.

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

Verifying the configuration

Ping the gateway from Host A and Host B. Both ping operations succeed.

Configuration files

```
#
 dot1x
#
vlan 1
 arp detection enable
#
interface Ten-GigabitEthernet1/0/1
 arp detection trust
#
interface Ten-GigabitEthernet1/0/2
 dot1x
#
interface Ten-GigabitEthernet1/0/3
 dot1x
#
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$3$M3ApC/8M0vqwqRqWukgESAeNIOr8zLg=
 key accounting cipher $c$3$819qOFvL68kuvygzU7vAIsfBdKEH4UgK
 retry 5
 timer response-timeout 5
 timer realtime-accounting 15
#
user-name-format without-domain
#
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

#
domain default enable aabbcc.net
#
local-user localuser class network
 password cipher $c$3$uDtqEKnjzk8dyJJ1h/gW3NapYpErpYtNoE4Pig==
 service-type lan-access
#
```

ARP configuration examples

This chapter provides ARP configuration examples.

Example: Configuring a static ARP entry

Applicable product matrix

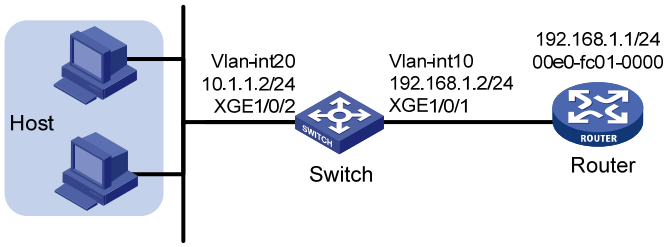
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 40:

- 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 40 Network diagram



Configuration procedures

Create VLAN 10.

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

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

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] port access vlan 10
[Switch-Ten-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 Ten-GigabitEthernet 1/0/2 to VLAN 20.

```
[Switch] interface ten-gigabitethernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] port access vlan 20
[Switch-Ten-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 that has IP address 192.168.1.1, MAC address 00e0-fc01-0000, and output interface Ten-GigabitEthernet 1/0/1 in VLAN 10.

```
[Switch] arp static 192.168.1.1 00e0-fc01-0000 10 ten-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       XGE1/0/1                N/A   S
10.1.1.1         0023-895f-958c  20       XGE1/0/2                3     D
10.1.1.5         000f-e234-5679  20       XGE1/0/2                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 Ten-GigabitEthernet1/0/1
 port access vlan 10
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 20
#
```

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

Example: Configuring a multiport ARP entry

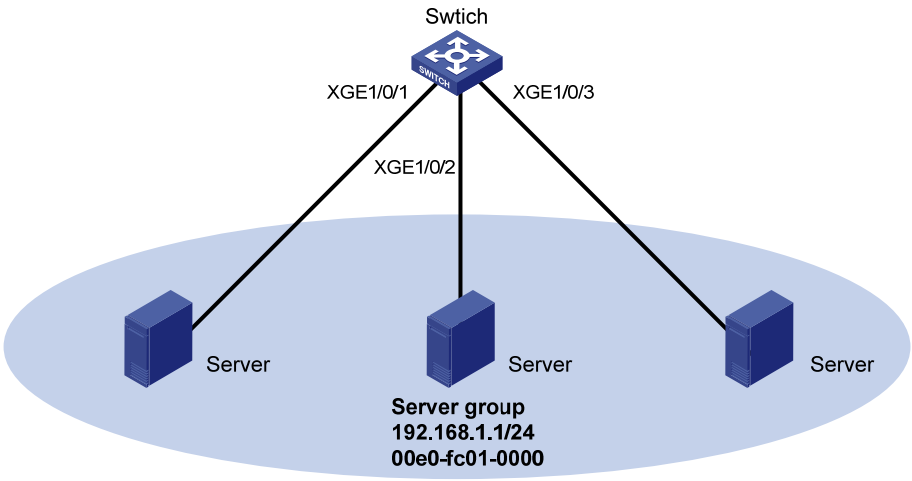
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 41, configure a multiport ARP entry on the switch to send packets destined for 192.168.1.1 to the three servers in VLAN 10.

Figure 41 Network diagram



Configuration procedures

Create VLAN 10.

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

Add interfaces Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to VLAN 10.

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] port access vlan 10
[Switch-Ten-GigabitEthernet1/0/1] quit
[Switch] interface ten-gigabitethernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] port access vlan 10
[Switch-Ten-GigabitEthernet1/0/2] quit
```

```
[Switch] interface ten-gigabitethernet 1/0/3
[Switch-Ten-GigabitEthernet1/0/3] port access vlan 10
[Switch-Ten-GigabitEthernet1/0/3] 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
```

Add a multiport unicast MAC address entry. The entry has MAC address 00e0-fc01-0000, and output interfaces Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet1/0/3 in VLAN 10.

```
[Switch] mac-address multiport 00e0-fc01-0000 interface Ten-GigabitEthernet 1/0/1 to
Ten-GigabitEthernet 1/0/3 vlan 10
```

Configure a multiport ARP entry that contains IP address 192.168.1.1 and MAC address 00e0-fc01-0000 in VLAN 10.

```
[Switch] arp multiport 192.168.1.1 00e0-fc01-0000 10
```

Verifying the configuration

Display all ARP entries on the switch.

```
[Switch] display arp
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP address       MAC address     VLAN     Interface              Aging Type
192.168.1.1      00e0-fc01-0000  10       N/A                    N/A   M
```

Configuration files

```
#
vlan 10
#
interface Vlan-interface10
 ip address 192.168.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 10
#
interface Ten-GigabitEthernet1/0/2
port access vlan 10
#
interface Ten-GigabitEthernet1/0/3
port access vlan 10
#
mac-address multiport 00e0-fc01-0000 interface Ten-GigabitEthernet1/0/1 to
Ten-GigabitEthernet1/0/3 vlan 10
#
arp multiport 192.168.1.1 00e0-fc01-0000 10
#
```

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 they would on 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

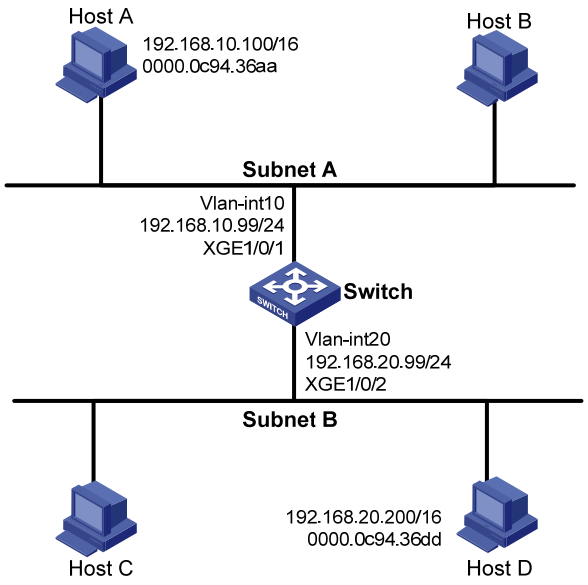
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 42, configure common proxy ARP on the switch to enable communication between Host A and Host D.

Figure 42 Network diagram



Configuration procedures

Create VLAN 10.

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

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

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] port access vlan 10
[Switch-Ten-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 Ten-GigabitEthernet 1/0/2 to VLAN 20.

```
[Switch] interface ten-gigabitethernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] port access vlan 20
[Switch-Ten-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 Ten-GigabitEthernet1/0/1
 port access vlan 10
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 20
#
```

Example: Configuring local proxy ARP

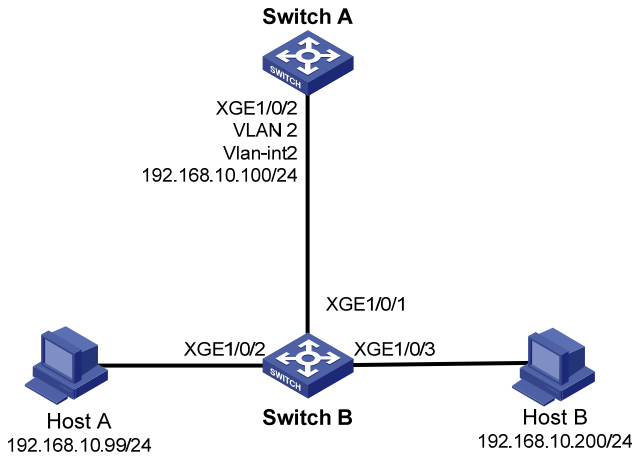
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 43, 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 43 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 ten-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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port ten-gigabitethernet 1/0/1
[SwitchB-vlan2] port ten-gigabitethernet 1/0/2
[SwitchB-vlan2] port ten-gigabitethernet 1/0/3
[SwitchB-vlan2] quit
```

   # Create isolation group 1.

```
<SwitchB> system-view
[SwitchB] port-isolate group 1
```

   # Assign Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 to isolation group 1.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port-isolate enable group 1
[SwitchB-Ten-GigabitEthernet1/0/2] quit
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port-isolate enable group 1
[SwitchB-Ten-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:
Group ID: 1
 Group members:
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet1/0/3
```

Ping Host B from Host A. The ping operation succeeds. Layer 3 communication is effective.

Disable local proxy ARP on Switch A, and then ping Host B from Host A. The ping operation fails. Layer 2 isolation 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 Ten-GigabitEthernet1/0/2
 port access vlan 2
#
```

- Switch B:

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

#

BGP configuration examples

This chapter provides BGP configuration examples.

Example: Configuring basic BGP

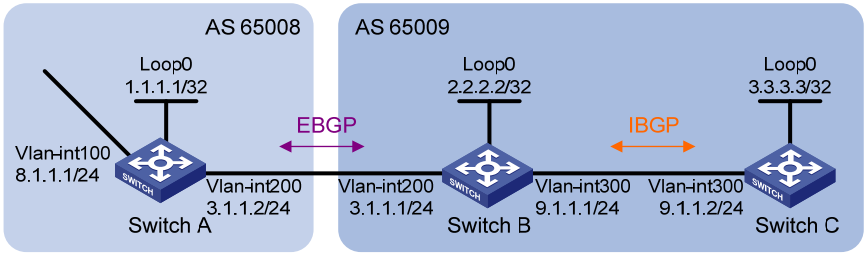
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 44, run EBGP between Switch A and Switch B, and run IBGP between Switch B and Switch C so that Switch C can access the network 8.1.1.0/24 connected to Switch A.

Figure 44 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To prevent route flapping caused by port state changes, this example uses loopback interfaces to establish IBGP connections. Loopback interfaces are virtual interfaces. Use the **peer connect-interface** command to specify the loopback interface as the source interface for establishing BGP connections. Enable OSPF in AS 65009 to make sure Switch B can communicate with Switch C through loopback interfaces.
- The EBGP peers, Switch A and Switch B (which usually belong to different carriers), are located in different ASs. Typically, their loopback interfaces are not reachable to each other, so their directly connected interfaces are used to establish BGP sessions. To enable Switch C to access the network 8.1.1.0/24 directly connected to Switch A, inject network 8.1.1.0/24 to the BGP routing table of Switch A.

Configuration procedures

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IBGP:

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 3.3.3.3 as-number 65009
[SwitchB-bgp] peer 3.3.3.3 connect-interface loopback 0
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-ipv4] peer 3.3.3.3 enable
[SwitchB-bgp-ipv4] quit
[SwitchB-bgp] quit
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 9.1.1.1 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

   # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 2.2.2.2 as-number 65009
[SwitchC-bgp] peer 2.2.2.2 connect-interface loopback 0
[SwitchC-bgp] ipv4-family unicast
[SwitchC-bgp-ipv4] peer 2.2.2.2 enable
[SwitchC-bgp-ipv4] quit
[SwitchC-bgp] quit
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

   # Display BGP peer information on Switch C.

```
[SwitchC] display bgp peer ipv4

BGP local router ID : 3.3.3.3
 Local AS number : 65009
 Total number of peers : 1                 Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2.2.2.2              65009        2        2    0       0 00:00:13 Established
```

   The output shows that Switch C has established an IBGP peer relationship with Switch B.

3. Configure EBGP:

Configure Switch A.

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 3.1.1.1 as-number 65009
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-ipv4] peer 3.1.1.1 enable
[SwitchA-bgp-ipv4] network 8.1.1.0 24
[SwitchA-bgp-ipv4] quit
[SwitchA-bgp] quit
```

Configure Switch B.

```
[SwitchB] bgp 65009
[SwitchB-bgp] peer 3.1.1.2 as-number 65008
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-ipv4] peer 3.1.1.2 enable
[SwitchB-bgp-ipv4] quit
[SwitchB-bgp] quit
```

Display BGP peer information on Switch B.

```
[SwitchB] display bgp peer ipv4

 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 2                 Peers in established state : 2

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  3.3.3.3              65009        4        4    0       0 00:02:49 Established
  3.1.1.2              65008        2        2    0       0 00:00:05 Established
```

The output shows that Switch B has established an IBGP peer relationship with Switch C and an EBGP peer relationship with Switch A.

Display the BGP routing table on Switch A.

```
[SwitchA] display bgp routing-table ipv4

 Total number of routes: 1

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

  >  8.1.1.0/24         8.1.1.1         0                     0       i
```

Display the BGP routing table on Switch B.

```
[SwitchB] display bgp routing-table ipv4
```

```
 Total number of routes: 1

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

  >e 8.1.1.0/24         3.1.1.2         0                     0       65008i
```

Display the BGP routing table on Switch C.

```
[SwitchC] display bgp routing-table ipv4

 Total number of routes: 1

 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

    i 8.1.1.0/24        3.1.1.2         0          100        0       65008i
```

The outputs show that Switch A has not learned any route to AS 65009. Switch C has learned the route to network 8.1.1.0, but the next hop 3.1.1.2 is unreachable. Therefore, the route is invalid.

4. Redistribute direct routes:

Configure BGP to redistribute direct routes on Switch B, so that Switch A can learn the route to 9.1.1.0/24, and Switch C can learn the route to 3.1.1.0/24.

Configure Switch B.

```
[SwitchB] bgp 65009
[SwitchB-bgp] ipv4-family unicast
[SwitchB-bgp-ipv4] import-route direct
[SwitchB-bgp-ipv4] quit
[SwitchB-bgp] quit
```

Display the BGP routing table on Switch A.

```
[SwitchA] display bgp routing-table ipv4

 Total number of routes: 4

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

  >e 2.2.2.2/32         3.1.1.1         0                     0       65009?
```

```
   e 3.1.1.0/24         3.1.1.1         0                    0       65009?
  >  8.1.1.0/24         8.1.1.1         0                    0       i
  >e 9.1.1.0/24         3.1.1.1         0                    0       65009?
```

The output shows that two routes (2.2.2.2/32 and 9.1.1.0/24) have been added into Switch A's routing table.

Display the BGP routing table on Switch C.

```
[SwitchC] display bgp routing-table ipv4

 Total number of routes: 4

 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

    Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

  i 2.2.2.2/32         2.2.2.2         0          100        0       ?
 >i 3.1.1.0/24         2.2.2.2         0          100        0       ?
 >i 8.1.1.0/24         3.1.1.2         0          100        0       65008i
 >i 9.1.1.0/24         2.2.2.2         0          100        0       ?
```

The output shows that the route 8.1.1.0 becomes valid with the next hop as Switch A.

Verifying the configuration

Ping 8.1.1.1 from Switch C.

```
[SwitchC] ping 8.1.1.1
PING 8.1.1.1 (8.1.1.1): 56 data bytes
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms
--- 8.1.1.1 ping statistics ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.000/4.800/10.000/2.638 ms
```

Configuration files

- Switch A:

```
#
vlan 100
#
vlan 200
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
```

```
#
interface Vlan-interface100
 ip address 8.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 3.1.1.2 255.255.255.0
#
bgp 65008
router-id 1.1.1.1
peer 3.1.1.1 as-number 65009
#
ipv4-family unicast
network 8.1.1.0 255.255.255.0
peer 3.1.1.1 enable
#
```

- Switch B:

```
#
vlan 200
#
vlan 300
#
 interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface200
ip address 3.1.1.1 255.255.255.0
#
interface Vlan-interface300
ip address 9.1.1.1 255.255.255.0
#
bgp 65009
router-id 2.2.2.2
peer 3.1.1.2 as-number 65008
peer 3.3.3.3 as-number 65009
peer 3.3.3.3 connect-interface LoopBack0
#
ipv4-family unicast
import-route direct
peer 3.1.1.2 enable
peer 3.3.3.3 enable
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

- Switch C:

```
#
```

```
vlan 300
#
interface LoopBack0
ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface300
ip address 9.1.1.2 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
peer 2.2.2.2 as-number 65009
peer 2.2.2.2 connect-interface LoopBack0
#
ipv4-family unicast
peer 2.2.2.2 enable
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

Example: Configuring BGP GR

Applicable product matrix

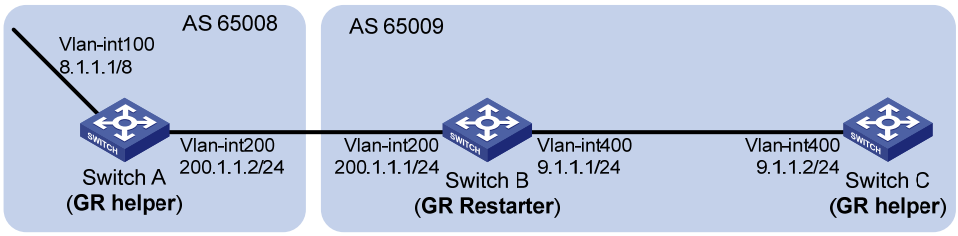
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 45, Switch B is an IRF fabric formed by two devices. It is connected to Switch A and Switch C through multichassis aggregate links.

Enable GR for BGP so that the communication between Switch A and Switch C is not affected when an active/standby switchover occurs on Switch B.

Figure 45 Network diagram



Configuration procedures

Configuring Switch A

Configure IP addresses for interfaces. (Details not shown.)

Configure the EBGP connection.

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
```

Enable GR capability for BGP.

```
[SwitchA-bgp] graceful-restart
```

Inject network 8.0.0.0/8 to the BGP routing table.

```
[SwitchA-bgp] ipv4-family
[SwitchA-bgp-ipv4] network 8.0.0.0
```

Enable Switch A to exchange IPv4 unicast routing information with Switch B.

```
[SwitchA-bgp-ipv4] peer 200.1.1.1 enable
```

Configuring Switch B

Configure IP addresses for interfaces. (Details not shown.)

Configure the EBGP connection.

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
```

Configure the IBGP connection.

```
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
```

Enable GR capability for BGP.

```
[SwitchB-bgp] graceful-restart
```

Inject networks 200.1.1.0/24 and 9.1.1.0/24 to the BGP routing table.

```
[SwitchB-bgp] ipv4-family
[SwitchB-bgp-ipv4] network 200.1.1.0 24
[SwitchB-bgp-ipv4] network 9.1.1.0 24
```

Enable Switch B to exchange IPv4 unicast routing information with Switch A and Switch C.

```
[SwitchB-bgp-ipv4] peer 200.1.1.2 enable
[SwitchB-bgp-ipv4] peer 9.1.1.2 enable
```

Configuring Switch C

Configure IP addresses for interfaces. (Details not shown.)

Configure the IBGP connection.

```
<SwitchC> system-view
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 9.1.1.1 as-number 65009
```

Enable GR capability for BGP.

```
[SwitchC-bgp] graceful-restart
```

Enable Switch C to exchange IPv4 unicast routing information with Switch B.

```
[SwitchC-bgp] ipv4-family
[SwitchC-bgp-ipv4] peer 9.1.1.1 enable
```

Verifying the configuration

Ping Switch C from Switch A. At the same time, perform an active/standby switchover on Switch B.

The ping operation is successful during the switchover process.

Configuration files

- Switch A:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 8.1.1.1 255.0.0.0
#
interface Vlan-interface200
ip address 200.1.1.2 255.0.0.0
#
bgp 65008
graceful-restart
router-id 1.1.1.1
peer 200.1.1.1 as-number 65009
#
ipv4-family unicast
network 8.0.0.0 255.0.0.0
peer 200.1.1.1 enable
#
```

- Switch B:

```
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
 ip address 200.1.1.1 255.255.255.0
#
interface Vlan-interface400
 ip address 9.1.1.1 255.255.255.0
#
bgp 65009
graceful-restart
```

```
router-id 2.2.2.2
peer 9.1.1.2 as-number 65009
peer 200.1.1.2 as-number 65008
#
ipv4-family unicast
network 9.1.1.0 255.255.255.0
network 200.1.1.0 255.255.255.0
peer 9.1.1.2 enable
peer 200.1.1.2 enable
#
```

- Switch C:

```
#
vlan 400
#
interface Vlan-interface400
ip address 9.1.1.2 255.255.255.0
#
bgp 65009
graceful-restart
router-id 3.3.3.3
peer 9.1.1.1 as-number 65009
#
ipv4-family unicast
peer 9.1.1.1 enable
#
```

Example: Configuring BFD for BGP

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 46, the switches in AS 200 run OSPF to reach each other. There are two paths between Switch A and Switch C: one over Switch B and the other over Switch D. When both paths are available, BGP uses the path over Switch B to forward traffic between Switch C and network 1.1.1.0/24.

Configure BFD for BGP on Switch A and Switch C to enable quick switchover to the path over Switch D when the path over Switch B fails.

Figure 46 Network diagram

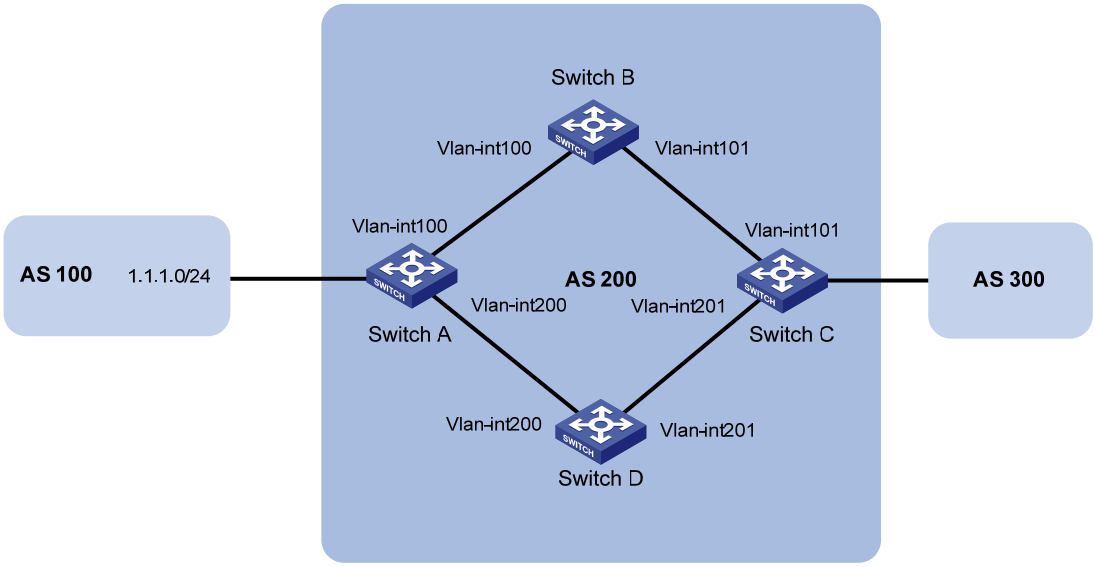


Table 3 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	3.0.1.1/24	Switch C	Vlan-int101	3.0.2.2/24
	Vlan-int200	2.0.1.1/24		Vlan-int201	2.0.2.2/24
Switch B	Vlan-int100	3.0.1.2/24	Switch D	Vlan-int200	2.0.1.2/24
	Vlan-int101	3.0.2.1/24		Vlan-int201	2.0.2.1/24

Configuration procedures

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure OSPF so that Switch A and Switch C can reach each other. (Details not shown.)
3. Configure IBGP on Switch A:

   # Establish two IBGP connections to Switch C.

```
<SwitchA> system-view
[SwitchA] bgp 200
[SwitchA-bgp] peer 3.0.2.2 as-number 200
[SwitchA-bgp] peer 2.0.2.2 as-number 200
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-ipv4] peer 3.0.2.2 enable
[SwitchA-bgp-ipv4] peer 2.0.2.2 enable
[SwitchA-bgp-ipv4] quit
[SwitchA-bgp] quit
```

   # Create ACL 2000 to permit network 1.1.1.0/24.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

Create two routing policies: **apply_med_50** and **apply_med_100**. Policy **apply_med_50** sets the MED to 50, and policy **apply_med_100** sets the MED to 100.

```
[SwitchA] route-policy apply_med_50 permit node 10
[SwitchA-route-policy-apply_med_50-10] if-match ip address acl 2000
[SwitchA-route-policy-apply_med_50-10] apply cost 50
[SwitchA-route-policy-apply_med_50-10] quit
[SwitchA] route-policy apply_med_100 permit node 10
[SwitchA-route-policy-apply_med_100-10] if-match ip address acl 2000
[SwitchA-route-policy-apply_med_100-10] apply cost 100
[SwitchA-route-policy-apply_med_100-10] quit
```

Apply **apply_med_50** to routes advertised to peer 3.0.2.2.

```
[SwitchA] bgp 200
[SwitchA-bgp] ipv4-family unicast
[SwitchA-bgp-ipv4] peer 3.0.2.2 route-policy apply_med_50 export
```

Apply **apply_med_100** to routes advertised to peer 2.0.2.2.

```
[SwitchA-bgp-ipv4] peer 2.0.2.2 route-policy apply_med_100 export
[SwitchA-bgp-ipv4] quit
```

Enable BFD for peer 3.0.2.2.

```
[SwitchA-bgp] peer 3.0.2.2 bfd
[SwitchA-bgp] quit
```

4. Configure IBGP on Switch C:

Establish two IBGP connections to Switch A.

```
<SwitchC> system-view
[SwitchC] bgp 200
[SwitchC-bgp] peer 3.0.1.1 as-number 200
[SwitchC-bgp] peer 2.0.1.1 as-number 200
[SwitchC-bgp] ipv4-family unicast
[SwitchC-bgp-ipv4] peer 3.0.1.1 enable
[SwitchC-bgp-ipv4] peer 2.0.1.1 enable
[SwitchC-bgp-ipv4] quit
```

Enable BFD for peer 3.0.1.1.

```
[SwitchC-bgp] peer 3.0.1.1 bfd
[SwitchC-bgp] quit
[SwitchC] quit
```

5. Configure EBGP on Switch A. (Details not shown.)

Verifying the configuration

Display detailed BFD session information on Switch C.

```
<SwitchC> display bfd session verbose

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

      Local Discr: 513                 Remote Discr: 513
```

```
        Source IP: 3.0.2.2           Destination IP: 3.0.1.1
    Session State: Up                     Interface: N/A
     Min Tx Inter: 500ms                Act Tx Inter: 500ms
     Min Rx Inter: 500ms                Detect Inter: 2500ms
         Rx Count: 135                      Tx Count: 135
     Connect Type: Indirect           Running Up for: 00:00:58
        Hold Time: 2457ms                  Auth mode: None
      Detect Mode: Async                        Slot: 0
         Protocol: BGP
        Diag Info: No Diagnostic
```

The output shows that a BFD session has been established between Switch A and Switch C.

Display BGP peer information on Switch C.

```
<SwitchC> display bgp peer ipv4

 BGP local router ID: 3.3.3.3
 Local AS number: 200
 Total number of peers: 2                 Peers in established state: 2

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2.0.1.1                200        4        5    0       0 00:01:55 Established
  3.0.1.1                200        4        5    0       0 00:01:52 Established
```

The output shows that Switch C has established two BGP connections in Established state with Switch A.

Display route 1.1.1.0/24 on Switch C.

```
<SwitchC> display ip routing-table 1.1.1.0 24 verbose

Summary Count : 1

Destination: 1.1.1.0/24
   Protocol: BGP             Process ID: 0
  SubProtID: 0x1                    Age: 00h00m09s
       Cost: 50               Preference: 255
        Tag: 0                     State: Active Adv
  OrigTblID: 0x1                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NBRID: 0x15000001          LastAs: 0
     AttrID: 0x1                Neighbor: 3.0.1.1
      Flags: 0x10060          OrigNextHop: 3.0.1.1
      Label: NULL             RealNextHop: 3.0.2.1
    BkLabel: NULL               BkNextHop: N/A
  Tunnel ID: Invalid            Interface: Vlan-interface101
BkTunnel ID: Invalid          BkInterface: N/A
```

The output shows that Switch C forwards packets destined for network 1.1.1.0/24 through the path Switch C<—>Switch B<—>Switch A.

Enable debugging on Switch C. When the path Switch C<—>Switch B<—>Switch A fails, the output shows the following:

```
<SwitchC> debugging bgp event
<SwitchC> terminal monitor
<SwitchC> terminal logging level 7
%Mar 12 19:02:59:241 2012 SwitchC BFD/6/FSM: -VDC=1; Sess[3.0.2.2/3.0.1.1, LD/RD:
513/513, Interface:N/A, SessType:Ctrl, LinkType:INET], Sta: UP->DOWN, Diag: 1
*Mar 12 19:02:59:242 2012 SwitchC BGP/7/DEBUG: -VDC=1;
 BGP.: 3.0.1.1 Receive ManualStop event in ESTABLISHED state.

*Mar 12 19:02:59:242 2012 SwitchC BGP/7/DEBUG: -VDC=1;
 BGP.: 3.0.1.1 Send NOTIFICATION
 Err/SubErr: 6/0 (Cease/ErrSubCode Unspecified)
 Error data NULL.

*Mar 12 19:02:59:243 2012 SwitchC BGP/7/DEBUG: -VDC=1;
 BGP.: 3.0.1.1 State is changed from ESTABLISHED to IDLE.
```

The output shows that Switch C can quickly detect the link failure and notify BGP to change the corresponding IBGP session state.

Display route 1.1.1.0/24 on Switch C.

```
<SwitchC> display ip routing-table 1.1.1.0 24 verbose

Summary Count : 1

Destination: 1.1.1.0/24
   Protocol: BGP             Process ID: 0
  SubProtID: 0x1                    Age: 00h03m08s
       Cost: 100            Preference: 255
        Tag: 0                    State: Active Adv
  OrigTblID: 0x1               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x15000000         LastAs: 0
     AttrID: 0x0               Neighbor: 2.0.1.1
      Flags: 0x10060        OrigNextHop: 2.0.1.1
      Label: NULL           RealNextHop: 2.0.2.1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface201
BkTunnel ID: Invalid        BkInterface: N/A
```

The output shows that Switch C forwards packets destined for network 1.1.1.0/24 through the path Switch C<—>Switch D<—>Switch A.

Configuration files

- Switch A:

```
#
vlan 100
#
vlan 200
#
```

```
interface Vlan-interface100
 ip address 3.0.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.0.1.2 255.255.255.0
#
bgp 200
router-id 1.1.1.1
peer 3.0.2.2 as-number 200
peer 2.0.2.2 as-number 200
peer 3.0.2.2 bfd
#
ipv4-family unicast
peer 3.0.2.2 enable
peer 2.0.2.2 enable
peer 3.0.2.2 route-policy apply_med_50 export
peer 2.0.2.2 route-policy apply_med_100 export
#
acl number 2000
rule permit source 1.1.1.0 0.0.0.255
#
route-policy apply_med_50 permit node 10
if-match ip address acl 2000
apply cost 50
#
route-policy apply_med_100 permit node 10
if-match ip address acl 2000
apply cost 100
#
ospf 1
area 0.0.0.0
network 3.0.1.1 0.0.0.255
network 2.0.1.1 0.0.0.255
#
```

- Switch B:

```
#
vlan 100
#
vlan 101
#
interface Vlan-interface100
ip address 3.0.1.2 255.255.255.0
#
interface Vlan-interface101
ip address 3.0.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
```

```
network 3.0.1.2 0.0.0.255
network 3.0.2.1 0.0.0.255
#
```

- Switch C:

```
#
vlan 101
#
vlan 201
#
interface Vlan-interface101
ip address 3.0.2.2 255.255.255.255
#
interface Vlan-interface201
ip address 2.0.2.2 255.255.255.0
#
bgp 200
router-id 3.3.3.3
peer 3.0.1.1 as-number 200
peer 2.0.1.1 as-number 200
peer 3.0.1.1 bfd
#
ipv4-family unicast
peer 3.0.1.1 enable
peer 2.0.1.1 enable
#
ospf 1
area 0.0.0.0
network 3.0.2.2 0.0.0.255
network 2.0.2.2 0.0.0.255
#
```

- Switch D:

```
#
vlan 200
#
vlan 201
#
interface Vlan-interface200
ip address 2.0.1.2 255.255.255.255
#
interface Vlan-interface201
ip address 2.0.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 2.0.1.2 0.0.0.255
network 2.0.2.1 0.0.0.255
#
```

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.

Example: Configuring CFD

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

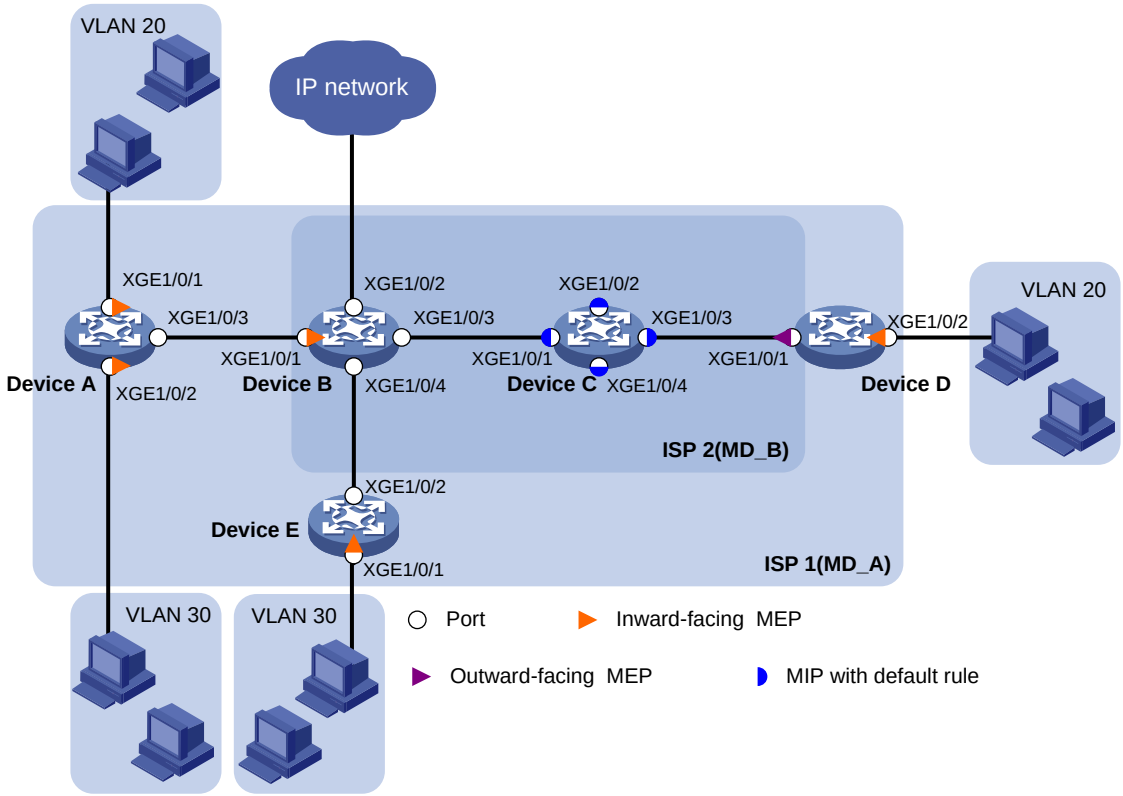
Network requirements

As shown in Figure 47:

- Device A, Device D, and Device E are managed by ISP 1.
- Device B and Device C are managed by ISP 2.

Configure CFD to implement link connectivity detection, fault verification, and fault location.

Figure 47 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

In this example, the MAC addresses of Device A through Device E are 0010-FC00-6511, 0010-FC00-6512, 0010-FC00-6513, 0010-FC00-6514, and 0010-FC00-6515, respectively.

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

As shown in Figure 47, create VLANs on the devices and assign ports to the VLANs. (Details not shown.)

Configuring service instances

Based on the MAs to which the MEPs belong, perform the configurations 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 service instance 1 (in which the MA is named **MA_A_1** and serves VLAN 20).

   ```
   [DeviceA] cfd service-instance 1 ma-id string MA_A_1 md MD_A vlan 20
   ```

   # Create service instance 2 (in which the MA is named **MA_A_2** and serves VLAN 30).

   ```
   [DeviceA] cfd service-instance 2 ma-id string MA_A_2 md MD_A vlan 30
   ```

   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 service-instance 3 ma-id string MA_B_1 md MD_B vlan 20
   ```

3. Configure Device C:

   ```
   [DeviceC] cfd md MD_B level 3
   [DeviceC] cfd service-instance 3 ma-id string MA_B_1 md MD_B vlan 20
   ```

4. Configure Device D:

   ```
   [DeviceD] cfd md MD_A level 5
   [DeviceD] cfd service-instance 1 ma-id string MA_A_1 md MD_A vlan 20
   [DeviceD] cfd md MD_B level 3
   [DeviceD] cfd service-instance 3 ma-id string MA_B_1 md MD_B vlan 20
   ```

5. Configure Device E:

```
[DeviceE] cfd md MD_A level 5
[DeviceE] cfd service-instance 2 ma-id string MA_A_2 md MD_A vlan 30
```

Configuring MEPs

Assign MEP IDs as described in the following table:

Service instance	Device	Port	MEP ID	MEP type
1	Device A	Ten-GigabitEthernet 1/0/1	1001	Inward-facing MEP
	Device D	Ten-GigabitEthernet 1/0/2	1002	Inward-facing MEP
2	Device A	Ten-GigabitEthernet 1/0/2	2001	Inward-facing MEP
	Device E	Ten-GigabitEthernet 1/0/1	2002	Inward-facing MEP
3	Device B	Ten-GigabitEthernet 1/0/1	3001	Inward-facing MEP
	Device D	Ten-GigabitEthernet 1/0/1	3002	Outward-facing MEP

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 inward-facing MEP 1001 in service instance 1 on Ten-GigabitEthernet 1/0/1.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Create inward-facing MEP 2001 in service instance 2 on Ten-GigabitEthernet 1/0/2.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 inbound
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure Device B in the same way Device A is configured:

   ```
   [DeviceB] cfd meplist 3001 3002 service-instance 3
   [DeviceB] interface ten-gigabitethernet 1/0/1
   [DeviceB-Ten-GigabitEthernet1/0/1] cfd mep 3001 service-instance 3 inbound
   [DeviceB-Ten-GigabitEthernet1/0/1] quit
   ```

3. Configure Device D in the same way Device A is configured:

   ```
   [DeviceD] cfd meplist 1001 1002 service-instance 1
   [DeviceD] cfd meplist 3001 3002 service-instance 3
   [DeviceD] interface ten-gigabitethernet 1/0/2
   [DeviceD-Ten-GigabitEthernet1/0/2] cfd mep 1002 service-instance 1 inbound
   [DeviceD-Ten-GigabitEthernet1/0/2] quit
   [DeviceD] interface ten-gigabitethernet 1/0/1
   [DeviceD-Ten-GigabitEthernet1/0/1] cfd mep 3002 service-instance 3 outbound
   [DeviceD-Ten-GigabitEthernet1/0/1] quit
   ```

4. Configure Device E in the same way Device A is configured:

   ```
   [DeviceE] cfd meplist 2001 2002 service-instance 2
   [DeviceE] interface ten-gigabitethernet 1/0/1
   [DeviceE-Ten-GigabitEthernet1/0/1] cfd mep 2002 service-instance 2 inbound
   [DeviceE-Ten-GigabitEthernet1/0/1] quit
   ```

Configuring a MIP generation rule

MIP configuration is optional. MIPs process LTM frames and LBM frames, and they can help implement link fault identification and location.

Configure the MIP generation rule in service instance 3 on Device C as **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 Ten-GigabitEthernet 1/0/1.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Enable the sending of CCM frames for MEP 2001 in service instance 2 on Ten-GigabitEthernet 1/0/2.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure Device B in the same way Device A is configured:

   ```
   [DeviceB] interface ten-gigabitethernet 1/0/1
   [DeviceB-Ten-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3001 enable
   [DeviceB-Ten-GigabitEthernet1/0/1] quit
   ```

3. Configure Device D in the same way Device A is configured:

   ```
   [DeviceD] interface ten-gigabitethernet 1/0/1
   [DeviceD-Ten-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3002 enable
   [DeviceD-Ten-GigabitEthernet1/0/1] interface ten-gigabitethernet 1/0/2
   [DeviceD-Ten-GigabitEthernet1/0/2] cfd cc service-instance 1 mep 1002 enable
   [DeviceD-Ten-GigabitEthernet1/0/2] quit
   ```

4. Configure Device E in the same way Device A is configured:

   ```
   [DeviceE] interface ten-gigabitethernet 1/0/1
   [DeviceE-Ten-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 2002 enable
   [DeviceE-Ten-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
Sent: 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 3001-43462:
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 index 1 level 5
 cfd service-instance 1 ma-id string MA_A_1 ma-index 1 md MD_A vlan 20
 cfd meplist 1001 to 1002 service-instance 1
 cfd service-instance 2 ma-id string MA_A_2 ma-index 1 md MD_A vlan 30
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 20
#
vlan 30
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 20
 cfd mep 1001 service-instance 1 inbound
 cfd cc service-instance 1 mep 1001 enable
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 30
 cfd mep 2001 service-instance 2 inbound
 cfd cc service-instance 2 mep 2001 enable
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 20 30
```

- Device B:

```
#
 cfd enable
```

```
 cfd md MD_B index 1 level 3
 cfd service-instance 3 ma-id string MA_B_1 ma-index 1 md MD_B vlan 20
 cfd meplist 3001 to 3002 service-instance 3
#
vlan 20
#
vlan 30
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 20 30
 cfd mep 3001 service-instance 3 inbound
 cfd cc service-instance 3 mep 3001 enable
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 20 30
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 20
#
interface Ten-GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 30
```

- Device C:

```
#
 cfd enable
 cfd md MD_B index 1 level 3
 cfd service-instance 3 ma-id string MA_B_1 ma-index 1 md MD_B vlan 20
 cfd mip-rule default service-instance 3
#
vlan 20
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 20
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 20
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 20
#
interface Ten-GigabitEthernet1/0/4
 port link-type trunk
```

```
 port trunk permit vlan 20
```

- Device D:

```
#
 cfd enable
 cfd md MD_A index 1 level 5
 cfd md MD_B index 2 level 3
 cfd service-instance 1 ma-id string MA_A_1 ma-index 1 md MD_A vlan 20
 cfd meplist 1001 to 1002 service-instance 1
 cfd service-instance 3 ma-id string MA_B_1 ma-index 1 md MD_B vlan 20
 cfd meplist 3001 to 3002 service-instance 3
#
vlan 20
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 20
 cfd mep 3002 service-instance 3 outbound
 cfd cc service-instance 3 mep 3002 enable
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 20
 cfd mep 1002 service-instance 1 inbound
 cfd cc service-instance 1 mep 1002 enable
```

- Device E:

```
#
 cfd enable
 cfd md MD_A index 1 level 5
 cfd service-instance 2 ma-id string MA_A_2 ma-index 1 md MD_A vlan 30
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 30
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 30
 cfd mep 2002 service-instance 2 inbound
 cfd cc service-instance 2 mep 2002 enable
#
interface Ten-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

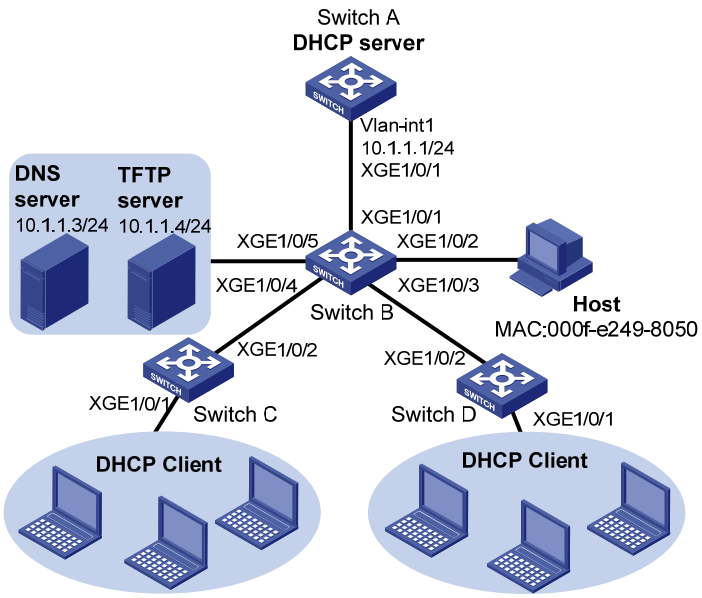
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 48, configure the DHCP server on Switch A to implement the following:

- Dynamically assign IP addresses on subnet 10.1.1.0/24 to DHCP clients.
- Dynamically assign IP addresses from 10.1.1.100 to 10.1.1.150 to devices of a specific vendor according to Option 60 in the DHCP requests.
- Assign a fixed IP address to the host according to its MAC address.
- Assign other configuration parameters including DNS server address, TFTP server address, and gateway address to DHCP clients.

Figure 48 Network diagram



Requirements analysis

To make sure the DNS server address and the TFTP server address are not assigned to any client by the DHCP server, you must exclude them from dynamic address allocation.

Configuration restrictions and guidelines

HP recommends that you configure the subnet where the interface of the DHCP server or DHCP relay agent resides as the subnet for dynamic allocation. This ensures correct address allocation.

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
[SwitchA-Vlan-interface1] quit
```

Enable DHCP.

```
[SwitchA] dhcp enable
```

Enable DHCP server on VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp select server
[SwitchA-Vlan-interface1] quit
```

Exclude the DNS server address and the TFTP server address from dynamic address allocation.

```
[SwitchA] dhcp server forbidden-ip 10.1.1.3
[SwitchA] dhcp server forbidden-ip 10.1.1.4
```

Create DHCP user class **aa** and configure a rule to match client requests with Option 60.

```
[SwitchA] dhcp class aa
[SwitchA-dhcp-class-aa] if-match option 60 hex 4850 offset 0 length 3
[SwitchA-dhcp-class-aa] quit
```

Configure DHCP address pool 0.

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5 hardware-address 000f-e249-8050
[SwitchA-dhcp-pool-0] dns-list 10.1.1.3
[SwitchA-dhcp-pool-0] tftp-server ip-address 10.1.1.4
[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] address range 10.1.1.6 10.1.1.100
[SwitchA-dhcp-pool-1] class aa range 10.1.1.100 10.1.1.150
[SwitchA-dhcp-pool-1] tftp-server ip-address 10.1.1.4
```

```
[SwitchA-dhcp-pool-1] dns-list 10.1.1.3
[SwitchA-dhcp-pool-1] domain-name com
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.1
[SwitchA-dhcp-pool-1] quit
```

Configuring Switch B

Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address dhcp-alloc
[SwitchB-Vlan-interface1] quit
```

Configuring Switch C

Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address dhcp-alloc
[SwitchC-Vlan-interface1] quit
```

Configuring Switch D

Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 1
[SwitchD-Vlan-interface1] ip address dhcp-alloc
[SwitchD-Vlan-interface1] quit
```

Verifying the configuration

Verify that the DHCP clients can obtain IP addresses and all other configuration parameters from Switch A.

Configuration files

- Switch A:

```
#
 dhcp enable
 dhcp server forbidden-ip 10.1.1.3
 dhcp server forbidden-ip 10.1.1.4
#
vlan 1
#
dhcp class aa
 if-match option 60 hex 483343 offset 2 length 3
#
dhcp server ip-pool 0
 dns-list 10.1.1.3
 domain-name com
 gateway-list 10.1.1.1
```

```
 static-bind ip-address 10.1.1.5 mask 255.0.0.0 hardware-address 000f-e249-8050
 tftp-server ip-address 10.1.1.4
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
 address range 10.1.1.6 10.1.1.100
 class aa range 10.1.1.100 10.1.1.150
 dns-list 10.1.1.3
 domain-name com
 gateway-list 10.1.1.1
 tftp-server ip-address 10.1.1.4
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
#
```

- Switch B:

```
#
vlan 1
#
interface Vlan-interface1
 ip address dhcp-alloc
#
```

- Switch C:

```
#
vlan 1
#
interface Vlan-interface1
 ip address dhcp-alloc
#
```

- Switch D:

```
#
vlan 1
#
interface Vlan-interface1
 ip address dhcp-alloc
#
```

Example: Configuring the DHCP relay agent

Applicable product matrix

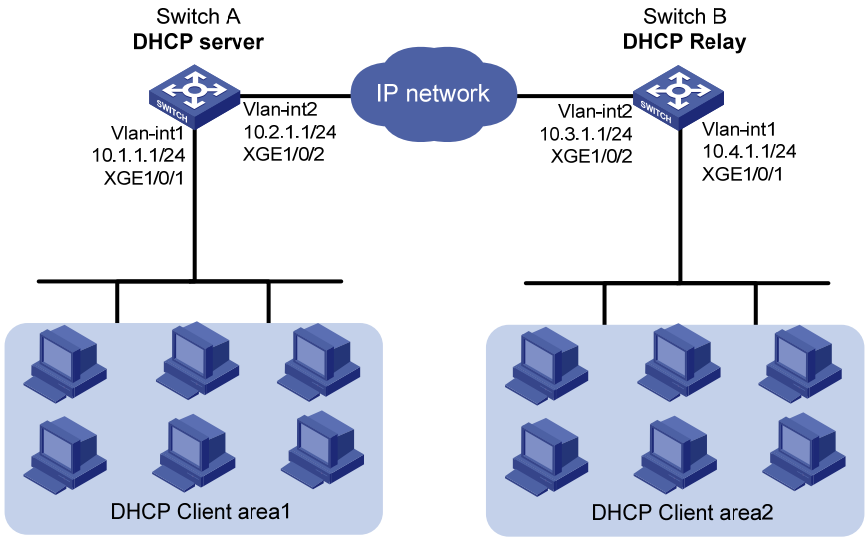
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 49, Switch A and Switch B can reach each other.

- Configure the DHCP server on Switch A to assign IP addresses to clients in area 1.
- Configure the DHCP relay agent on Switch B to implement the following:
  - The DHCP server can assign IP addresses to DHCP clients in area 2.
  - DHCP clients in area 2 cannot use manually configured static IP addresses to communicate with the external network.

Figure 49 Network diagram



Requirements analysis

To prevent clients in area 2 from using manually configured IP addresses to access the external network, you must perform the following tasks:

- Enable the DHCP relay agent to record clients' IP-to-MAC bindings.
- Enable the IPv4 source guard function.

The configuration ensures that the DHCP relay agent can forward only packets that match the DHCP relay entries.

Configuration restrictions and guidelines

When you configure the DHCP relay agent, follow these restrictions and guidelines:

- You must configure an IP address pool that contains the IP address of the DHCP relay agent on the DHCP server. This ensures that the DHCP clients can obtain correct IP addresses through the DHCP relay agent.
- The DHCP server must not reside on the same subnet as the DHCP relay agent interface. Otherwise, the clients might fail to obtain IP addresses.

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 Ten-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 Ten-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
```

Enable the DHCP relay agent to record clients' IP-to-MAC bindings.

```
[SwitchB] dhcp relay client-information record
```

Enable the DHCP relay agent on VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] dhcp select relay
```

Specify DHCP server 10.2.1.1 for DHCP server group 1 on the DHCP relay agent.

```
[SwitchB-Vlan-interface1] dhcp relay server-address 10.2.1.1
[SwitchB-Vlan-interface1] quit
```

Enable the IPv4 source guard function.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip verify source ip-address mac-address
[SwitchB-Vlan-interface1] quit
```

Verifying the configuration

Use the **display dhcp relay server-address** command on Switch B to verify the DHCP server address configuration.

```
[SwitchB] display dhcp relay server-address
    Interface name                                  Server IP address
    Vlan1                                           10.2.1.1
```

Verify that the DHCP clients in area 1 and area 2 can obtain IP addresses from Switch A, and communicate with the external network. (Details not shown.)

Configure a static IP address for a client in area 2. Verify that it cannot use the static IP address to access the external network.

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 Ten-GigabitEthernet1/0/1
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
dhcp enable
#
```

- Switch B:

```
#
 dhcp enable
 dhcp relay client-information record
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 10.4.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-address 10.2.1.1
 ip verify source ip-address mac-address
#
interface Vlan-interface2
 ip address 10.3.1.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
```

Example: Configuring the DHCP relay agent to support Option 82

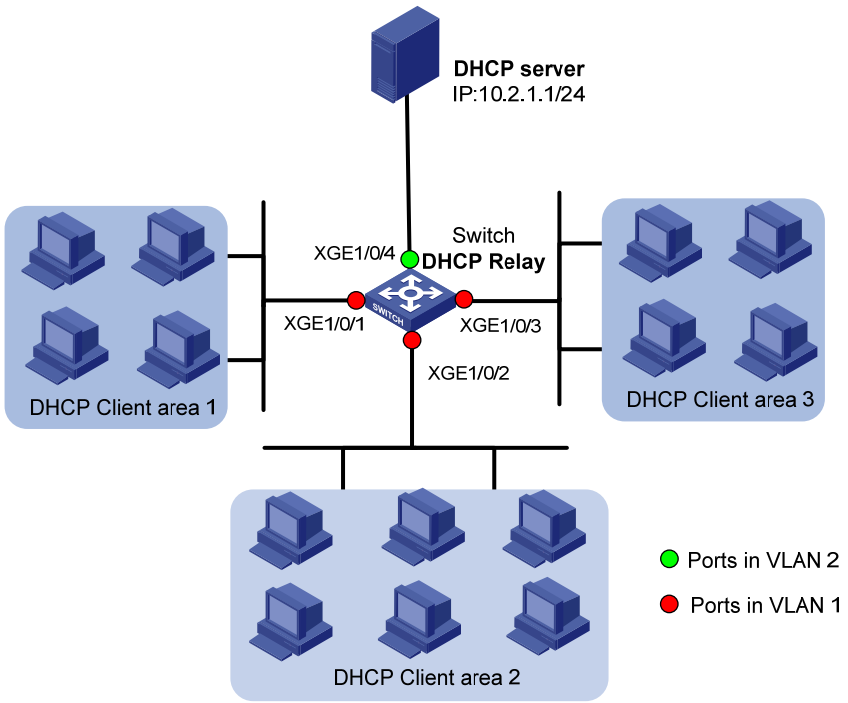
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 50, 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 different address ranges to DHCP clients in different areas.

Figure 50 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 Ten-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
```

Enable the DHCP relay agent on VLAN-interface 1.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] dhcp select relay
```

Specify DHCP server 10.2.1.1 for DHCP server group 1 on the DHCP relay agent.

```
[Switch-Vlan-interface1] dhcp relay server-address 10.2.1.1
```

Enable the DHCP relay agent to support Option 82.

```
[Switch-Vlan-interface1] dhcp relay information enable
```

Verifying the configuration

Verify that DHCP clients can obtain IP addresses in specific address ranges from the DHCP server. (Details not shown.)

Use the **display dhcp relay information** command to display Option 82 configuration on the DHCP relay agent.

```
[Switch] display dhcp relay information
Interface: Vlan-interface1
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: Normal
   Remote ID Pattern: Normal
   Circuit ID format: Hex
   Remote ID format: Hex
```

Configuration files

```
#
 dhcp enable
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
 dhcp select relay
 dhcp relay information enable
 dhcp relay server-address 10.2.1.1
#
interface Vlan-interface2
 ip address 10.2.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 2
#
```

Example: Configuring DHCP snooping

Applicable product matrix

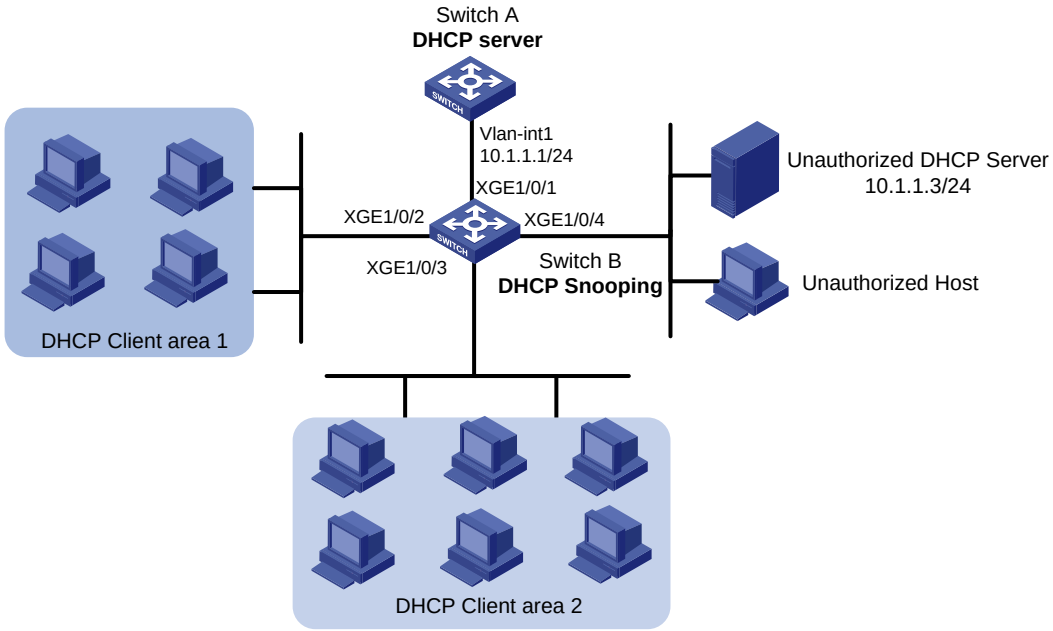
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 51, configure DHCP snooping on Switch B to implement the following:

- DHCP clients can obtain IP addresses from the authorized DHCP server (Switch A).
- DHCP clients cannot use static IP addresses to access the external network.

Figure 51 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Configure Ten-GigabitEthernet 1/0/1 connected to the authorized DHCP server as a trusted port. This port can forward responses from the authorized DHCP server to DHCP clients while other ports cannot.
- Enable ARP detection in VLAN 1 for user validity check to prevent users from accessing the network through static IP addresses.

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 enable
```

Specify Ten-GigabitEthernet 1/0/1 as a trusted port.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] dhcp snooping trust
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/2.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/3.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] dhcp snooping binding record
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/4.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/4
[SwitchB-Ten-GigabitEthernet1/0/4] dhcp snooping binding record
[SwitchB-Ten-GigabitEthernet1/0/4] quit
```

Enable ARP detection for user validity check.

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

Configure Ten-GigabitEthernet 1/0/1 facing the DHCP server as an ARP trusted port. By default, a port is an ARP untrusted port.

```
[SwitchB-vlan1] quit
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] arp detection trust
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display DHCP snooping entries.

```
[SwitchB] display dhcp snooping binding
1 DHCP snooping entries found.
 IP Address      MAC Address    Lease        VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 10.1.1.5        0023-8912-3d07 863963       1    N/A    XGE1/0/2
```

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 enable
#
vlan 1
 arp detection enable
#
interface Ten-GigabitEthernet1/0/1
 arp detection trust
 dhcp snooping trust
#
interface Ten-GigabitEthernet1/0/2
 dhcp snooping binding record
#
interface Ten-GigabitEthernet1/0/3
 dhcp snooping binding record
#
interface Ten-GigabitEthernet1/0/4
 dhcp snooping binding record
#
```

DLDP configuration examples

This document provides DLDP configuration examples.

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 5920	Release 2208P01
HP 5900	Release 2210

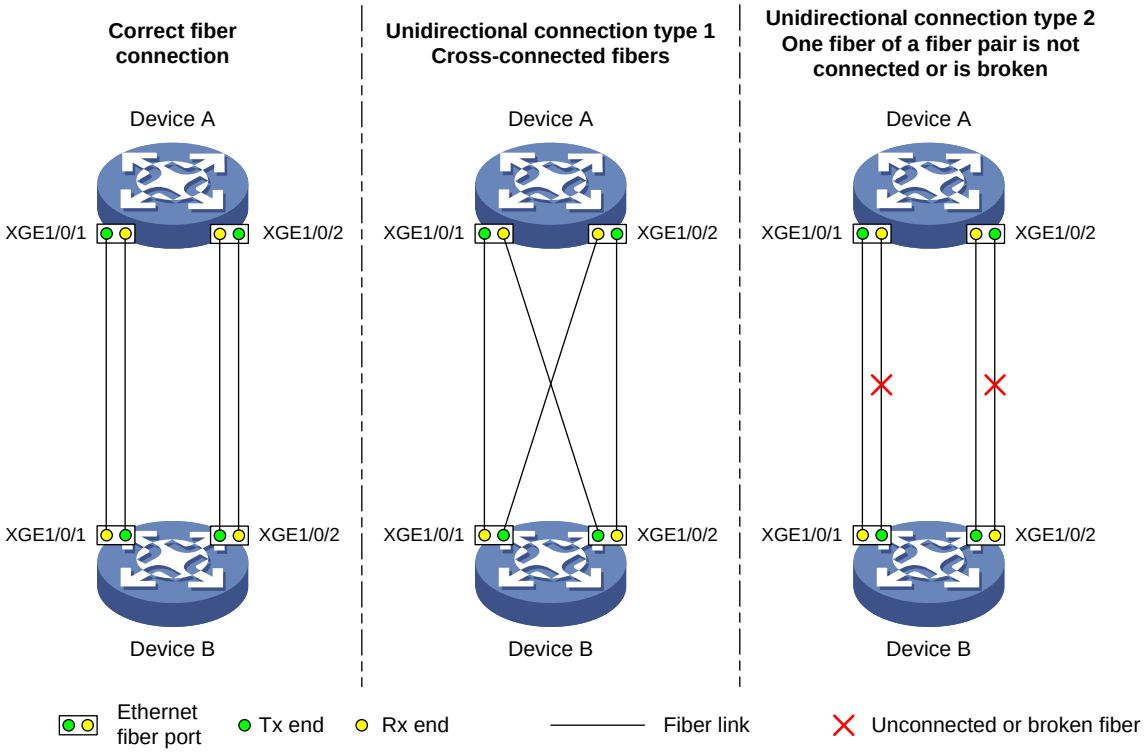
Network requirements

As shown in Figure 52, 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 52 Network diagram



Configuration 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.

Configuration procedures

1. Configure Device A:

   # Enable DLDP globally.

   ```
   <DeviceA> system-view
   [DeviceA] dldp global enable
   ```

   # Configure Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to operate in full duplex mode at 10000 Mbps, and enable DLDP on the ports.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] duplex full
   [DeviceA-Ten-GigabitEthernet1/0/1] speed 10000
   [DeviceA-Ten-GigabitEthernet1/0/1] dldp enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] duplex full
   [DeviceA-Ten-GigabitEthernet1/0/2] speed 10000
   [DeviceA-Ten-GigabitEthernet1/0/2] dldp enable
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   ```

   # 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

Display the DLDP configuration globally and for all the DLDP-enabled ports on Device A.

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface Ten-GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface Ten-GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

The output shows that both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are in Bidirectional state. Both links are bidirectional.

Enable the monitoring of logs on the current terminal on Device A. Set the lowest level of the logs that can be output to the current terminal to 6.

```
[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6
```

Cross-connect the fiber pairs between Device A and Device B. The following log information is displayed on Device A:

```
<DeviceA>%Jul 11 17:40:31:089 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/1
link status is DOWN.
%Jul 11 17:40:31:091 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/1 is DOWN.
%Jul 11 17:40:31:677 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is DOWN.
%Jul 11 17:40:31:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/2 is DOWN.
```

```
%Jul 11 17:40:38:544 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/1 link
status is UP.
%Jul 11 17:40:38:836 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is UP.
```

The output shows that the port status of both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 is down and then up, but the link status of them is always down.

Display the DLDP configuration globally and for all the DLDP-enabled ports on Device A.

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface Ten-GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)

Interface Ten-GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)
```

The output shows that the DLDP port status of both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 is unidirectional. This indicates that DLDP detects unidirectional links on them and automatically shuts down the two ports.

Correct the fiber connections. As a result, the ports shut down by DLDP automatically recover, and Device A displays the following log information:

```
<DeviceA>%Jul 11 17:42:57:709 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/1
link status is DOWN.
%Jul 11 17:42:58:603 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is DOWN.
%Jul 11 17:43:02:342 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/1 link
status is UP.
%Jul 11 17:43:02:343 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface Ten-GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and
the port index is 1.
%Jul 11 17:43:02:344 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface Ten-GigabitEthernet1/0/1.
%Jul 11 17:43:02:353 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/1 is UP.
%Jul 11 17:43:02:357 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is UP.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface Ten-GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and
the port index is 2.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface Ten-GigabitEthernet1/0/2.
%Jul 11 17:43:02:368 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/2 is UP.
```

The output shows that the port status and link status of both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are now up and their DLDP neighbors are determined.

Configuration files

- Device A:

```
#
dldp global enable
#
interface Ten-GigabitEthernet1/0/1
 speed 10000
 duplex full
 dldp enable
#
interface Ten-GigabitEthernet1/0/2
 speed 10000
 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 5920	Release 2208P01
HP 5900	Release 2210

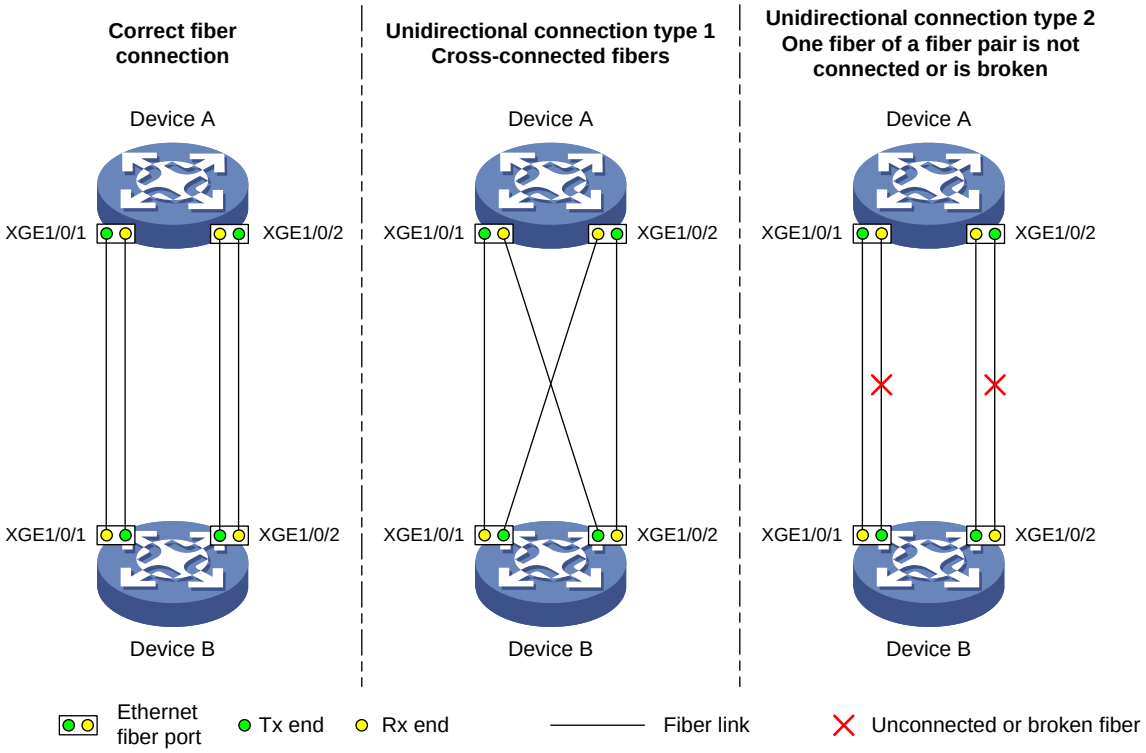
Network requirements

As shown in Figure 53, Device A and Device B are connected with two fiber pairs.

Configure DLDP on the devices to meet the following 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 53 Network diagram



Configuration 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.

Configuration procedures

1. Configure Device A:

   # Enable DLDP globally.

   ```
   <DeviceA> system-view
   [DeviceA] dldp global enable
   ```

   # Configure Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to operate in full duplex mode at 10000 Mbps. Enable DLDP on the ports.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] duplex full
   [DeviceA-Ten-GigabitEthernet1/0/1] speed 10000
   [DeviceA-Ten-GigabitEthernet1/0/1] dldp enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] duplex full
   [DeviceA-Ten-GigabitEthernet1/0/2] speed 10000
   [DeviceA-Ten-GigabitEthernet1/0/2] dldp enable
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   ```

   # 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

Display the DLDP configuration globally and on all the DLDP-enabled ports of Device A.

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface Ten-GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface Ten-GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

The output shows that both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are in Bidirectional state. Both links are bidirectional.

Enable the monitoring of logs on the current terminal on Device A. Set the lowest level of the logs that can be output to the current terminal to 6.

```
[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6
```

Cross-connect the fiber pairs between Device A and Device B. The following log information is displayed on Device A:

```
<DeviceA>%Jul 12 08:29:17:786 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/1
link status is DOWN.
%Jul 12 08:29:17:787 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/2 is DOWN.
```

```
%Jul 12 08:29:25:004 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/1 link
status is UP.
%Jul 12 08:29:25:005 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/1 is UP.
%Jul 12 08:29:25:893 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is UP.
%Jul 12 08:29:25:894 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/2 is UP.
```

The output shows that the port status and link status of both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are down and then up.

Display the DLDP configuration globally and for all the DLDP-enabled ports.

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface Ten-GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface Ten-GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

The output shows that the DLDP port status of both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 is unidirectional. This indicates that DLDP detects unidirectional links on them but does not shut down the two ports.

Shut down Ten-GigabitEthernet 1/0/1.

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-Ten-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2012 DeviceA IFNET/3/PHY_UPDOWN:
Ten-GigabitEthernet1/0/1 link status is DOWN.
%Jul 12 08:34:23:718 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:34:23:778 2012 DeviceA IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/2 link
status is DOWN.
%Jul 12 08:34:23:779 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/2 is DOWN.
```

The output shows that the port status and link status of both Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are now down.

Shut down Ten-GigabitEthernet 1/0/2.

```
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface ten-gigabitethernet 1/0/2
```

```
[DeviceA-Ten-GigabitEthernet1/0/2] shutdown
```

Correct the fiber connections, and bring up Ten-GigabitEthernet 1/0/2.

```
[DeviceA-Ten-GigabitEthernet1/0/2] undo shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-Ten-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2012 DeviceA IFNET/3/PHY_UPDOWN:
Ten-GigabitEthernet1/0/2 link status is UP.
%Jul 12 08:46:17:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/2 is UP.
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface Ten-GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and
the port index is 2.
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface Ten-GigabitEthernet1/0/2.
```

The output shows that the port status and link status of Ten-GigabitEthernet 1/0/2 are now up and its DLDP neighbors are determined.

Bring up Ten-GigabitEthernet1/0/1.

```
[DeviceA-Ten-GigabitEthernet1/0/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] undo shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-Ten-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2012 DeviceA IFNET/3/PHY_UPDOWN:
Ten-GigabitEthernet1/0/1 link status is UP.
%Jul 12 08:48:25:952 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed
on interface Ten-GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and
the port index is 1.
%Jul 12 08:48:25:953 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/1 is UP.
%Jul 12 08:48:25:953 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface Ten-GigabitEthernet1/0/1.
```

The output shows that the port status and link status of Ten-GigabitEthernet 1/0/1 are now up and its DLDP neighbors are determined.

Configuration files

- Device A:

```
#
 dldp global enable
 dldp unidirectional-shutdown manual
#
interface Ten-GigabitEthernet1/0/1
 speed 10000
 duplex full
 dldp enable
#
interface Ten-GigabitEthernet1/0/2
 speed 10000
 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.

Example: Configuring IPv4 static DNS

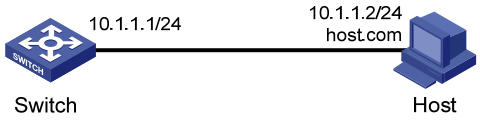
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 54, configure IPv4 static DNS so the switch can access the host by using the domain name **host.com** rather than an IP address.

Figure 54 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

Execute 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
  56 bytes from 10.1.1.2: icmp_seq=0 ttl=128 time=1.000 ms
  56 bytes from 10.1.1.2: icmp_seq=1 ttl=128 time=1.000 ms
  56 bytes from 10.1.1.2: icmp_seq=2 ttl=128 time=1.000 ms
  56 bytes from 10.1.1.2: icmp_seq=3 ttl=128 time=1.000 ms
  56 bytes from 10.1.1.2: icmp_seq=4 ttl=128 time=2.000 ms
-- host.com ping statistics ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.000/1.200/2.000/0.400 ms
```

Configuration files

```
#
 ip host host.com 10.1.1.2
#
```

Example: Configuring IPv4 dynamic DNS

Applicable product matrix

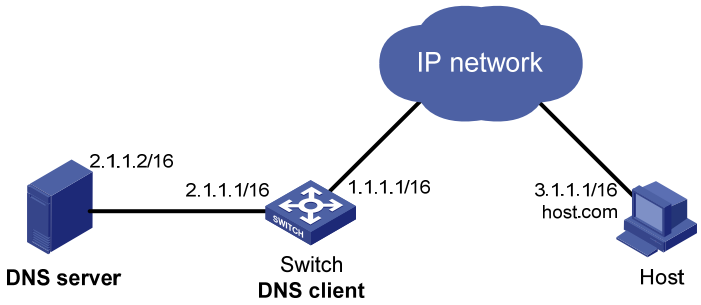
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 55, 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 55 Network diagram



Configuration procedures

Configuring the DNS server

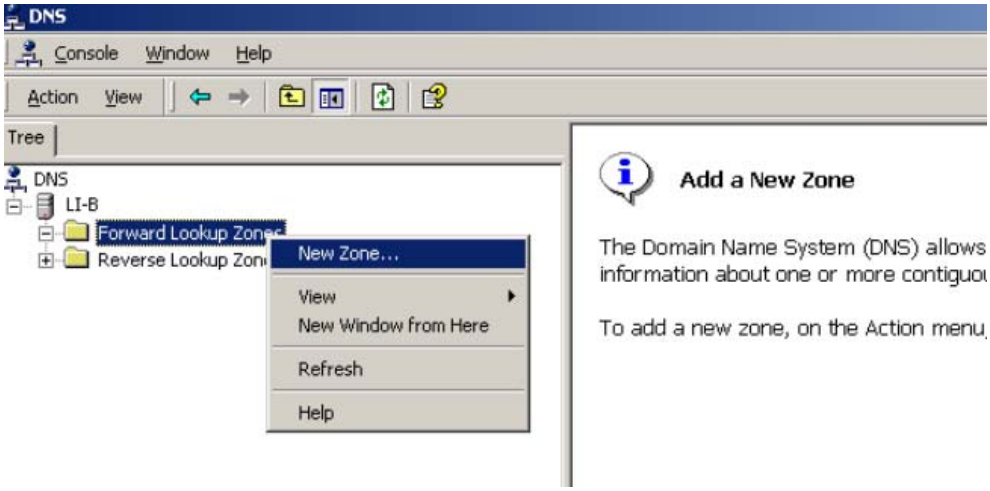
The configuration might vary with DNS servers. The following configuration is performed on a PC running Windows Server 2000.

1. Select **Start** > **Programs** > **Administrative Tools** > **DNS**.

   The DNS server configuration page appears, as shown in Figure 56.

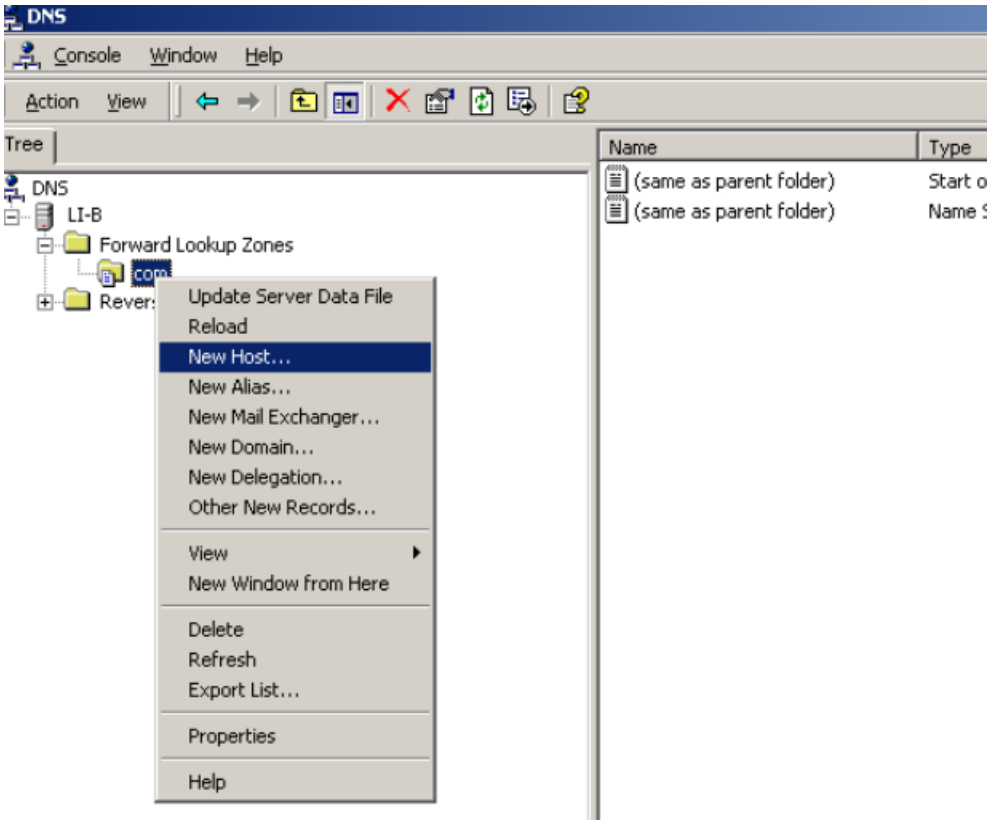
2. Right-click **Forward Lookup Zones**, select **New Zone**, and then follow the wizard to create a new zone named **com**.

Figure 56 Creating a zone



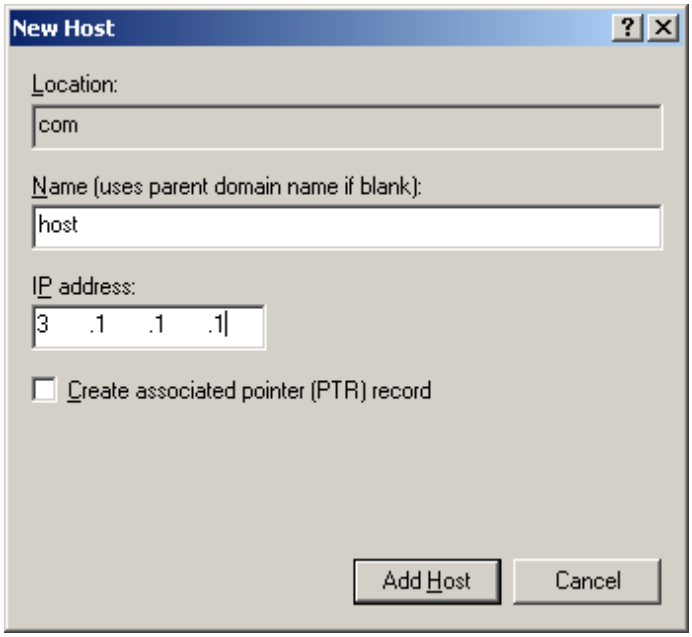
3. On the DNS server configuration page, right-click zone **com**, and select **New Host**.
   The new host configuration page appears, as shown in Figure 58.

Figure 57 Adding a host



4. 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 58 Adding a mapping between domain name and IP address



Configuring the DNS client

Specify the IP address of the DNS server as 2.1.1.2.

```
<Switch> system-view
[Switch] dns server 2.1.1.2
```

Specify **com** as the domain name suffix.

```
[Switch] dns domain com
```

Verifying the configuration

Execute 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
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=126 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=126 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=126 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=126 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=126 time=2.000 ms

--- Ping statistics for host ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

Configuration files

```
#
 dns server 2.1.1.2
 dns domain com
```

#

Example: Configuring IPv4 DNS

Applicable product matrix

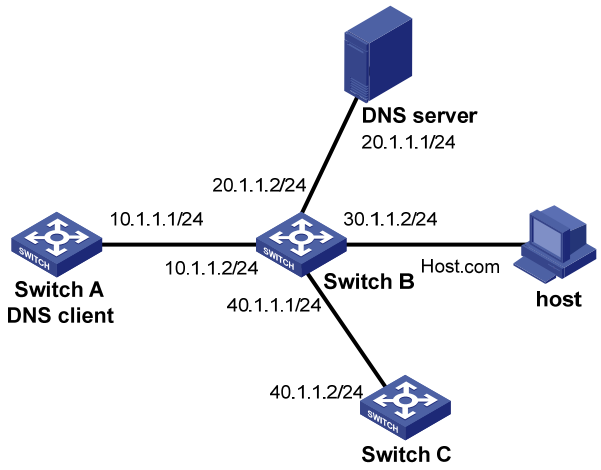
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 59, 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 DNS on Switch A so Switch A can access Switch C by using the domain name of Switch C.
- Configure dynamic DNS on Switch A so Switch A can access the host by using the domain name of the host.

Figure 59 Network diagram



Configuration procedures

Configuring the DNS server

For information about the DNS server configuration, see "Example: Configuring IPv4 dynamic DNS."

Configuring the DNS client

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
```

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

Execute 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
56 bytes from 40.1.1.2: icmp_seq=0 ttl=127 time=1.000 ms
56 bytes from 40.1.1.2: icmp_seq=1 ttl=127 time=1.000 ms
56 bytes from 40.1.1.2: icmp_seq=2 ttl=127 time=1.000 ms
56 bytes from 40.1.1.2: icmp_seq=3 ttl=127 time=1.000 ms
56 bytes from 40.1.1.2: icmp_seq=4 ttl=127 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

Execute 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 30.1.1.1.

```
[SwitchA] ping host
[SwitchA] ping host
Ping host.com (30.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 30.1.1.1: icmp_seq=0 ttl=127 time=1.000 ms
56 bytes from 30.1.1.1: icmp_seq=1 ttl=127 time=1.000 ms
56 bytes from 30.1.1.1: icmp_seq=2 ttl=127 time=1.000 ms
56 bytes from 30.1.1.1: icmp_seq=3 ttl=127 time=1.000 ms
56 bytes from 30.1.1.1: icmp_seq=4 ttl=127 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

Configuration files

```
#
 dns server 20.1.1.1
 dns domain com
#
ip host SwitchC 40.1.1.2
#
```

Example: Configuring IPv6 static DNS

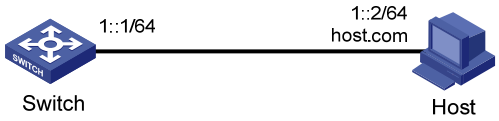
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 60, configure IPv6 static DNS so the switch can access the host by using the domain name **host.com** rather than an IPv6 address.

Figure 60 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
```

Verifying the configuration

Execute 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
Ping6(56 data bytes) 1::1 --> 1::2, press CTRL_C to break
56 bytes from 1::2, icmp_seq=0 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=1 hlim=128 time=0.000 ms
56 bytes from 1::2, icmp_seq=2 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=3 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=4 hlim=128 time=0.000 ms

--- Ping6 statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

Configuration files

```
#
```

```
 ipv6 host host.com 1::2
#
```

Example: Configuring IPv6 dynamic DNS

Applicable product matrix

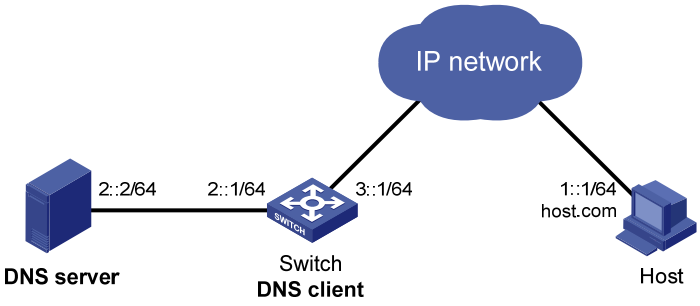
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 61, 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 61 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.

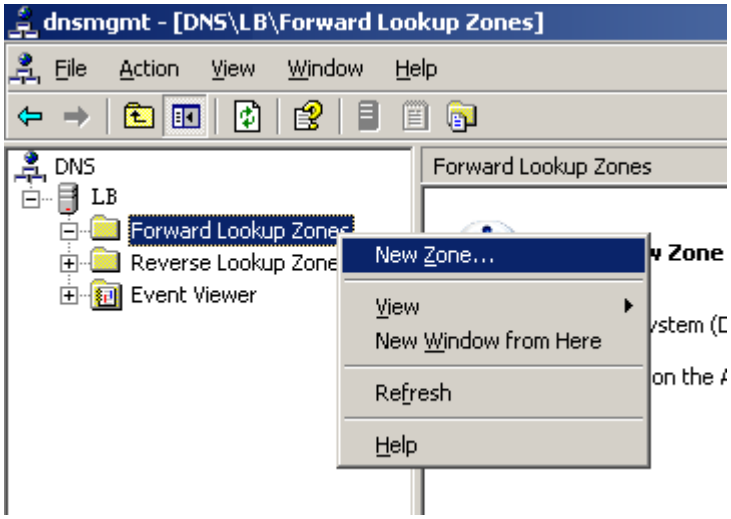
Make sure the DNS server supports IPv6 DNS, so that the server can process IPv6 DNS packets, and the interfaces of the DNS server can forward IPv6 packets.

1. Select **Start** > **Programs** > **Administrative Tools** > **DNS**.

   The DNS server configuration page appears, as shown in Figure 62.

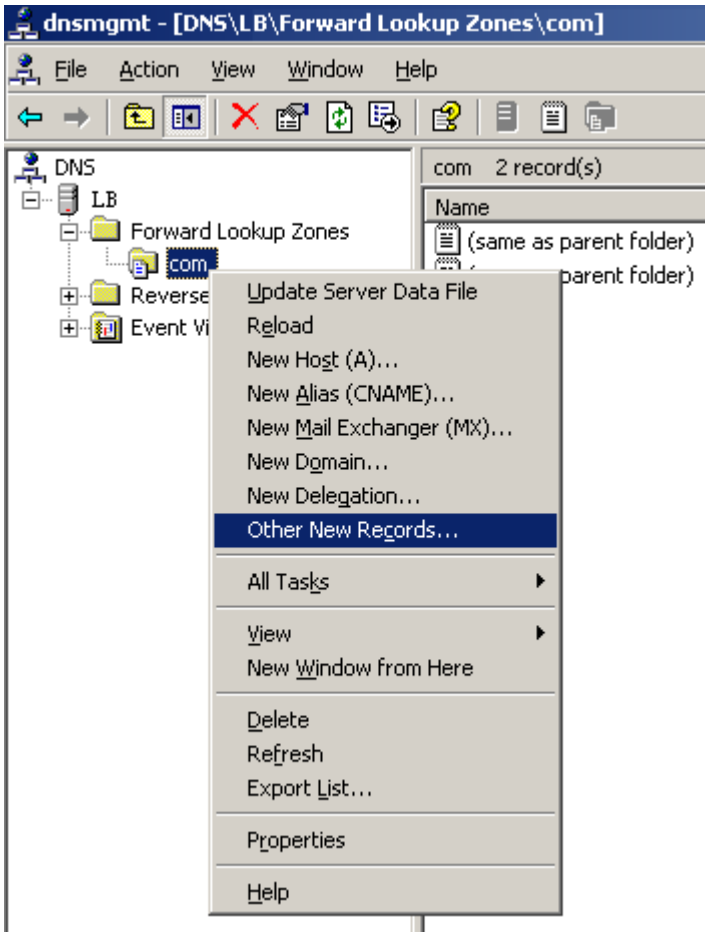
2. Right-click **Forward Lookup Zones**, select **New Zone**, and then follow the wizard to create a new zone named **com**.

Figure 62 Creating a zone



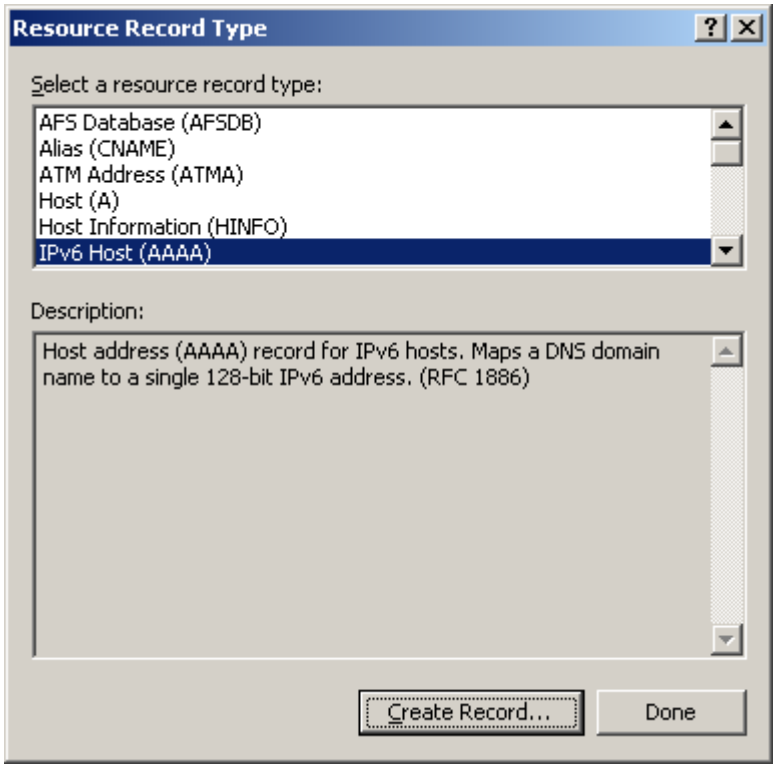
3. On the DNS server configuration page, right-click zone **com**, and select **Other New Records**. The resource record type configuration page appears, as shown in Figure 64.

Figure 63 Creating a record



4. Select **IPv6 Host (AAAA)** as the resource record type.

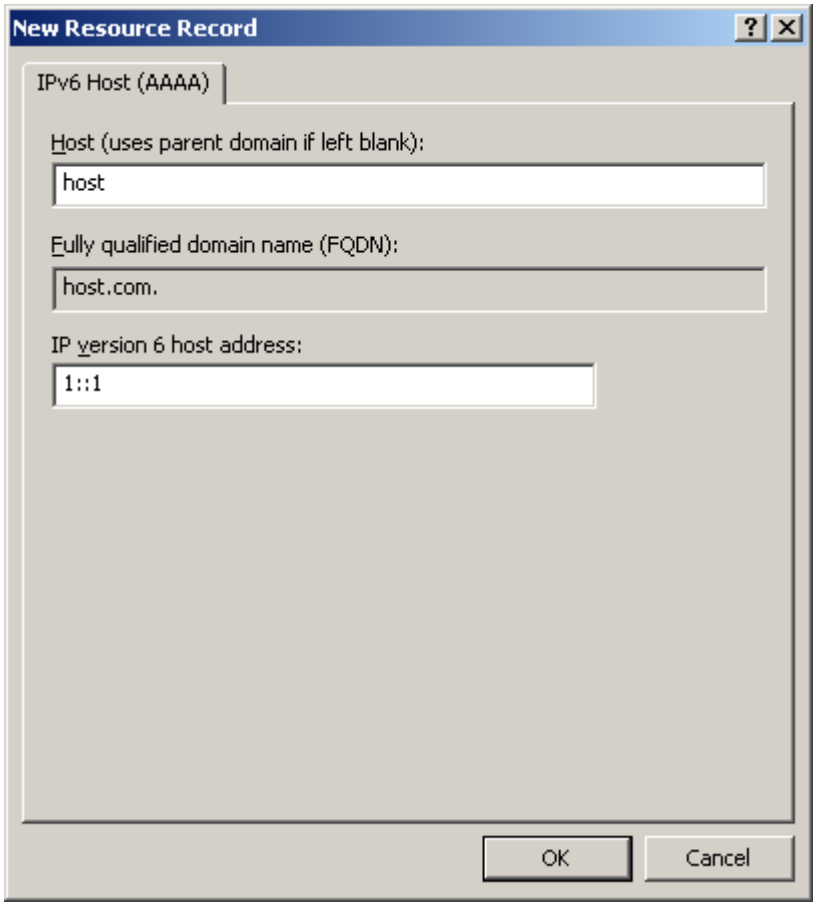
Figure 64 Selecting the resource record type



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 65 Adding a mapping between the domain name and IPv6 address



Configuring the DNS client

Specify the IP address of the DNS server as 2::2.

```
<Switch> system-view
[Switch] ipv6 dns server 2::2
```

Specify **com** as the DNS suffix.

```
[Switch] dns domain com
```

Verifying the configuration

Execute the **ping ipv6 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 1::1.

```
<Switch> ping ipv6 host
Ping6(56 data bytes) 3::1 --> 1::1, press CTRL_C to break
56 bytes from 1::1, icmp_seq=0 hlim=126 time=1.000 ms
56 bytes from 1::1, icmp_seq=1 hlim=126 time=0.000 ms
56 bytes from 1::1, icmp_seq=2 hlim=126 time=1.000 ms
56 bytes from 1::1, icmp_seq=3 hlim=126 time=1.000 ms
56 bytes from 1::1, icmp_seq=4 hlim=126 time=0.000 ms

--- Ping6 statistics for host ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

Configuration files

```
#
 dns domain com
 ipv6 dns server 2::2
#
```

Example: Configuring IPv6 DNS

Applicable product matrix

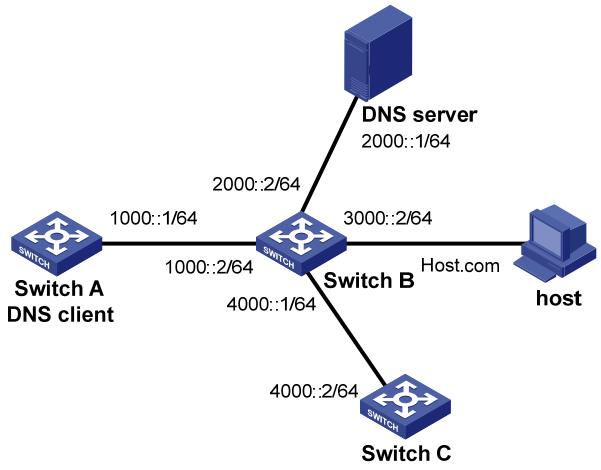
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

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 IPv6 address and access the host whose IPv6 address might change.

- Configure static DNS so Switch A can access Switch C by using the domain name of Switch C.
- Configure dynamic DNS so Switch A can 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 IPv6 dynamic DNS."

Configuring the DNS client

Create a mapping between IP address 4000::2 and domain name **SwitchC**.

```
<SwitchA> system-view
[SwitchA] ipv6 host SwitchC 4000::2
```

Specify the IP address of the DNS server as 2000::1.

```
[SwitchA] ipv6 dns server 2000::1
```

Specify **com** as the domain name suffix.

```
[SwitchA] dns domain com
```

Verifying the configuration

Execute 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
Ping6(56 data bytes) 1000::1 --> 4000::2, press CTRL_C to break
56 bytes from 4000::2, icmp_seq=0 hlim=127 time=1.000 ms
56 bytes from 4000::2, icmp_seq=1 hlim=127 time=0.000 ms
56 bytes from 4000::2, icmp_seq=2 hlim=127 time=1.000 ms
56 bytes from 4000::2, icmp_seq=3 hlim=127 time=1.000 ms
56 bytes from 4000::2, icmp_seq=4 hlim=127 time=0.000 ms

--- Ping6 statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

Execute 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
Ping6(56 data bytes) 1000::1 --> 3000::1, press CTRL_C to break
56 bytes from 3000::1, icmp_seq=0 hlim=126 time=1.000 ms
56 bytes from 3000::1, icmp_seq=1 hlim=126 time=0.000 ms
56 bytes from 3000::1, icmp_seq=2 hlim=126 time=1.000 ms
56 bytes from 3000::1, icmp_seq=3 hlim=126 time=1.000 ms
56 bytes from 3000::1, icmp_seq=4 hlim=126 time=0.000 ms

--- Ping6 statistics for host ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

Configuration files

```
#
 dns domain com
 ipv6 dns server 2000::1
#
ipv6 host SwitchC 4000::2
#
```

Emergency Shell Usage Examples

This chapter provides examples for using the emergency shell to load the system image when the system image does not exist or is corrupt.

Example: Using the emergency shell to load the system image

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 67, the switch has a boot image saved on its flash memory but does not have a system image. Use the emergency shell to download the correct system image from the TFTP server and load the image.

Figure 67 Network diagram

Usage restrictions and guidelines

When you use the emergency shell, follow these restrictions and guidelines:

- When the switch does not have a system image or the image is corrupt, you must connect to the device through the console port.
- After connecting to the device through the console port, reboot the switch to enter emergency shell. The prompt of the emergency shell is <boot>.

Usage procedures

Check which files are stored and how much space is available on the flash memory of the switch.

```
<boot> dir
Directory of flash:
   0 -rw-     1119363 Jan 01 2011 00:55:42   cmdtree.txt
   1 drw-           - Jan 01 2011 00:01:54   diagfile
```

```
   2 -rw-         567 Jan 01 2011 06:04:53   dsakey
   3 -rw-         735 Jan 01 2011 06:04:15   hostkey
   4 -rw-        1759 Jan 01 2011 01:39:49   ifindex.dat
   5 -rw-        3798 Jan 01 2011 01:39:49   irf.cfg
   6 -rw-       71892 Jan 01 2011 01:39:50   irf.mdb
   7 drw-           - Jan 01 2011 00:01:54   logfile
   8 -rw-    11261952 Oct 09 2013 17:05:33   5900_5920-cmw710-boot-r2210.bin
   9 drw-           - Jan 01 2011 00:01:54   seclog
  10 -rw-         591 Jan 01 2011 06:04:16   serverkey
  11 drw-           - Jan 01 2011 01:48:40   versionInfo

524288 KB total (309792 KB free)
```

The output shows the following information:

- The boot image **boot.bin** is present but the matching system image **system.bin** is not.
- The available space is 309792 KB, which is large enough for saving the system image **system.bin**.

Check the version information of the boot image.

```
<boot> display version
HP Comware Software, Version 7.1.035, Release 2210
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
HP 5900AF-48XG-4QSFP+ Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : Power on

Boot image: flash:/5900_5920-cmw710-boot-r2210.bin
Boot image version: 7.1.035

Slot 1
HP 5900AF-48XG-4QSFP+ Switch with 2 Processors
Last reboot reason : Power on
2048M   bytes SDRAM
4M      bytes Nor Flash Memory
512M    bytes Nand Flash Memory
Config Register points to Nand Flash
```

Configure an IP address and a gateway for the management Ethernet port.

```
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0] ip address 1.1.1.1 16
[boot-m-eth0] ip gateway 1.1.1.2
```

Verify that the switch and the TFTP server can reach each other.

```
<boot> ping 1.2.1.1
PING 1.2.1.1(1.2.1.1):56 data bytes
64 bytes from 1.2.1.1:seq=0 ttl=64 time=0.160 ms
64 bytes from 1.2.1.1:seq=1 ttl=64 time=0.062 ms
64 bytes from 1.2.1.1:seq=2 ttl=64 time=0.061 ms
64 bytes from 1.2.1.1:seq=3 ttl=64 time=0.065 ms
64 bytes from 1.2.1.1:seq=4 ttl=64 time=0.063 ms

--- 1.2.1.1 ping statistics ---
```

```
5 packets transmitted,5 packets received,0% packet loss
round-trip min/avg/max = 0.061/0.082/0.160 ms
```

Download the file **system.bin** from the TFTP server.

```
<boot> tftp 1.2.1.1 get system.bin flash:/5900_5920-cmw710-system-r2210.bin
```

Verify that the system image is compatible with the boot image.

```
<boot> display install package flash:/5900_5920-cmw710-system-r2210.bin
flash:/system.bin
  [Package]
  Vendor: HP
  Product: 5900_5920
  Service name: system
  Platform version: 7.1.035
  Product version: Release 2210
  Supported board: mpu
  [Component]
  Component: system
  Description: system package
```

Load the system image to start the Comware system.

```
<boot> install load flash:/5900_5920-cmw710-system-r2210.bin
Check package flash:/5900_5920-cmw710-system-r2210.bin ...

Extracting package ...

Loading...

User interface aux0 is available.


Press ENTER to get started.
```

Verifying the operation

Press **Enter**.

The prompt <*Device name*> appears, instead of the emergency shell prompt <boot>.

Display version information.

```
<Sysname>display version
HP Comware Software, Version 7.1.035, Release 2207
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
HP 5900AF-48XG-4QSFP+ Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : Power on

Boot image: flash:/5900_5920-cmw710-boot-r2210.bin
Boot image version: 7.1.035, Release 2210
System image: flash:/5900_5920-cmw710-system-r2210.bin
System image version: 7.1.035, Release 2210
```

```
---- More ----
```

The output shows that the switch has a system image now.

Configuration files

All commands used in this example are one-time commands and are not saved to the configuration file.

Ethernet OAM configuration examples

This document provides Ethernet OAM configuration examples.

Example: Configuring Ethernet OAM

Applicable product matrix

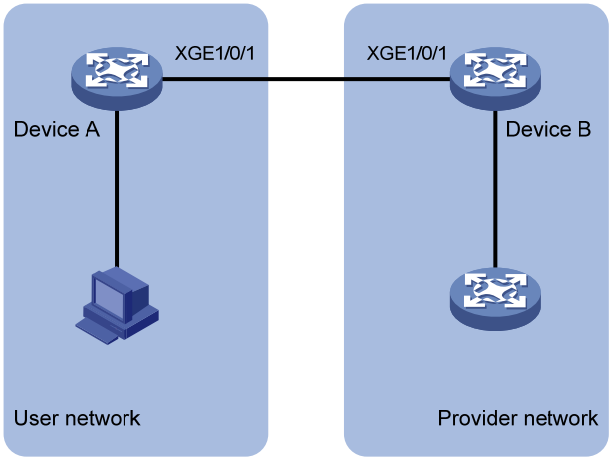
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 68, to satisfy the Service Level Agreement (SLA) for users, configure Ethernet OAM on edge switches Device A and Device B to meet these 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 68 Network diagram



Requirement analysis

To facilitate link detection for the provider, configure Ten-GigabitEthernet 1/0/1 on Device B to operate in active Ethernet OAM mode.

Configuration procedures

1. Configure Device A:

   # Configure Ten-GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode, and enable Ethernet OAM for it.

   ```
   <DeviceA> system-view
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] oam mode passive
   [DeviceA-Ten-GigabitEthernet1/0/1] oam enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

2. Configure Device B:

   # Configure Ten-GigabitEthernet 1/0/1 to operate in active Ethernet OAM mode. By default, all ports operate in active Ethernet OAM mode.

   ```
   <DeviceB> system-view
   [DeviceB] interface ten-gigabitethernet 1/0/1
   [DeviceB-Ten-GigabitEthernet1/0/1] oam mode active
   ```

   # Enable Ethernet OAM for the port.

   ```
   [DeviceB-Ten-GigabitEthernet1/0/1] oam enable
   [DeviceB-Ten-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Display the Ethernet OAM configuration on Device A.

```
[DeviceA] display oam configuration
---------------- [Global] ----------------
 OAM timers
   Hello timer        : 1000 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window           : 100 x 1000000 symbols
     Threshold        : 1 error symbols
   Errored frame
     Window           : 10 x 100 milliseconds
     Threshold        : 1 error frames
   Errored frame period
     Window           : 1000 x 10000 frames
     Threshold        : 1 error frames
   Errored frame seconds
     Window           : 600 x 100 milliseconds
     Threshold        : 1 error seconds
```

Display Ethernet OAM link event statistics of the remote end on Device B.

```
[DeviceB] display oam link-event remote
----------- [Ten-GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM remote errored frame event
```

```
Event time stamp        : 5789 x 100 milliseconds
Errored frame window    : 10 x 100 milliseconds
Errored frame threshold : 1 error frames
Errored frame           : 3 error frames
Error running total     : 35 error frames
Event running total     : 17 events
```

The output shows that 35 errors occurred on Device A since the Ethernet OAM connection was established, 17 of which were caused by error frames. The link is instable.

Configuration files

- Device A:

```
#
interface Ten-GigabitEthernet1/0/1
 oam mode passive
 oam enable
```

- Device B:

```
#
interface Ten-GigabitEthernet1/0/1
 oam enable
```

FCoE configuration examples

This chapter provides examples for building networks composed of FCoE switches in data centers.

General configuration restrictions and guidelines

When you configure FCoE, follow these restrictions and guidelines:

- The switch supports FCoE only when operating in advanced mode. For more information about system operating modes, see *Fundamentals Configuration Guide*.
- In an FCoE network, HP recommends that you set the delay for the IRF ports to report a link down event as 0 on IRF member devices. For more information, see the **irf link-delay** command in *Fundamentals Command Reference*.

Example: Building a fabric statically

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 69, configure Switch A and Switch B to build a fabric to meet the following requirements:

- Network flapping is avoided.
- SAN traffic can be transmitted on lossless Ethernet.
- The server can access the disk through the fabric.

Figure 69 Network diagram

Requirements analysis

To meet the network requirements, perform the following tasks:

- To avoid network flapping and adapt to the simple network topology, use the static method to build the fabric.

- To transmit SAN traffic on lossless Ethernet:
  - Configure DCBX, PFC in auto mode, and ETS on the Ethernet interface connecting the switch to the server.
  - Configure DCBX and PFC in auto mode on the Ethernet interface connecting the switch to the disk.
  - Forcibly enable PFC on the Ethernet interfaces connecting the two switches.

  For more information about configuring DCBX, PFC, and ETS, see *Layer 2—LAN Switching Configuration Guide*.
- To enable the server to access the disk, configure the members in the default zone to access each other.

Configuration restrictions and guidelines

When you build a fabric statically, follow these restrictions and guidelines:

- Make sure the fabric configuration function is disabled on all switches.
- The fabric name must be the same for all switches.
- The domain ID for each switch must be unique in the fabric.

Configuration procedures

Configuring Switch A

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchA> system-view
   [SwitchA] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchA] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchA] quit
   ```

   # Reboot the switch.

   ```
   <SwitchA> reboot
   Start to check configuration with next startup configuration file, please
   wait.........DONE!
   Current configuration will be lost after the reboot, save current configuration?
   [Y/N]:y
   ```

```
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

3. Configure DCBX:

   # Enable LLDP globally.

```
[SwitchA] lldp global enable
```

   # Create an Ethernet frame header ACL numbered 4000.

```
[SwitchA] acl number 4000 name DCBX
```

   # Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchA-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchA-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchA-acl-ethernetframe-4000] quit
```

   # Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchA] traffic classifier DCBX operator or
[SwitchA-classifier-DCBX] if-match acl 4000
[SwitchA-classifier-DCBX] quit
```

   # Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchA] traffic behavior DCBX
[SwitchA-behavior-DCBX] remark dot1p 3
[SwitchA-behavior-DCBX] quit
```

   # Create a QoS policy named **DCBX**.

```
[SwitchA] qos policy DCBX
```

   # Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchA-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
```

4. Configure PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

5. Configure ETS:

Configure the 802.1p-lp priority map to:

- Map 802.1p priority 3 to local precedence 1 (corresponding to queue 1).
- Map all other 802.1p priorities to local precedence 0 (corresponding to queue 0).

```
[SwitchA] qos map-table dot1p-lp
[SwitchA-maptbl-dot1p-lp] import 3 export 1
[SwitchA-maptbl-dot1p-lp] import 0 export 0
[SwitchA-maptbl-dot1p-lp] import 1 export 0
[SwitchA-maptbl-dot1p-lp] import 2 export 0
[SwitchA-maptbl-dot1p-lp] import 4 export 0
[SwitchA-maptbl-dot1p-lp] import 5 export 0
[SwitchA-maptbl-dot1p-lp] import 6 export 0
[SwitchA-maptbl-dot1p-lp] import 7 export 0
[SwitchA-maptbl-dot1p-lp] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/1 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

6. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchA] fcoe-mode fcf
[SwitchA] vsan 1
[SwitchA-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchA-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 1 in VSAN 1.

```
[SwitchA-vsan1] domain-id 1 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchA-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchA-Vfc1] port trunk vsan 1
[SwitchA-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchA] interface vfc 2
[SwitchA-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchA-Vfc2] port trunk vsan 1
[SwitchA-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 1
[SwitchA-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchA] vsan 1
[SwitchA-vsan1] zone default-zone permit
```

```
[SwitchA-vsan1] quit
```

Configuring Switch B

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchB> system-view
   [SwitchB] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchB] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchB] quit
   ```

   # Reboot the switch.

   ```
   <SwitchB> reboot
   Start to check configuration with next startup configuration file, please
   wait.........DONE!
   Current configuration will be lost after the reboot, save current configuration?
   [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   flash:/startup.cfg exists, overwrite? [Y/N]:y
   Validating file. Please wait...
   Configuration is saved to flash successfully.
   This command will reboot the device. Continue? [Y/N]:y
   Now rebooting, please wait...
   ```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

   ```
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
   [SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
   [SwitchB-Ten-GigabitEthernet1/0/1] quit
   ```

   # Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

   ```
   [SwitchB] interface ten-gigabitethernet 1/0/2
   [SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
   ```

```
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

3. Configure DCBX:

   # Enable LLDP globally.

```
[SwitchB] lldp global enable
```

   # Create an Ethernet frame header ACL numbered 4000.

```
[SwitchB] acl number 4000 name DCBX
```

   # Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchB-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchB-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchB-acl-ethernetframe-4000] quit
```

   # Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchB] traffic classifier DCBX operator or
[SwitchB-classifier-DCBX] if-match acl 4000
[SwitchB-classifier-DCBX] quit
```

   # Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchB] traffic behavior DCBX
[SwitchB-behavior-DCBX] remark dot1p 3
[SwitchB-behavior-DCBX] quit
```

   # Create a QoS policy named **DCBX**.

```
[SwitchB] qos policy DCBX
```

   # Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchB-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchB-qospolicy-DCBX] quit
```

   # Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchB-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

   # Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
```

4. Configuring PFC:

   # Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

   # Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

   # Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

   # Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

5. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchB] fcoe-mode fcf
[SwitchB] vsan 1
[SwitchB-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchB-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 2 in VSAN 1.

```
[SwitchB-vsan1] domain-id 2 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchB-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchB] interface vfc 1
[SwitchB-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchB-Vfc1] port trunk vsan 1
[SwitchB-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchB] interface vfc 2
[SwitchB-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchB-Vfc2] port trunk vsan 1
[SwitchB-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchB] vlan 10
[SwitchB-vlan10] fcoe enable vsan 1
[SwitchB-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchB] vsan 1
[SwitchB-vsan1] zone default-zone permit
[SwitchB-vsan1] quit
```

Verifying the configuration

Display the domain information on Switch A for VSAN 1.

```
[SwitchA] display fc domain vsan 1
Domain Information of VSAN 1:

    Running time information:
        State: Stable
        Switch WWN: 48:33:43:2d:46:43:1A:1A
        Fabric name: 11:11:11:11:11:11:11:11
        Priority: 128
        Domain ID: 1
    Configuration information:
        Domain configure: Disabled
        Domain auto-reconfigure: Disabled
        Fabric name: 11:11:11:11:11:11:11:11
        Priority: 128
        Domain ID: 1 (static)
    Principal switch running time information:
        Priority: 128

    No interfaces available.
```

The output shows that:

- The domain configuration on Switch A is completed.
- The runtime domain ID for Switch A is 1.

Display the domain information on Switch B for VSAN 1.

```
[SwitchB] display fc domain vsan 1
Domain Information of VSAN 1:

    Running time information:
        State: Stable
        Switch WWN: 48:33:43:2d:46:43:1B:1B
        Fabric name: 11:11:11:11:11:11:11:11
        Priority: 128
        Domain ID: 2
    Configuration information:
        Domain configure: Disabled
        Domain auto-reconfigure: Disabled
        Fabric name: 11:11:11:11:11:11:11:11
        Priority: 128
        Domain ID: 2 (static)
    Principal switch running time information:
        Priority: 128

    No interfaces available.
```

The output shows that:

- The domain configuration on Switch B is completed.
- The runtime domain ID for Switch B is 2.

Configuration files

- Switch A:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 1 static
 undo domain configure enable
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
```

```
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

- Switch B:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 2 static
 undo domain configure enable
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
traffic classifier DCBX operator or
 if-match acl 4000
#
```

```
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

Example: Building a fabric dynamically

Applicable product matrix

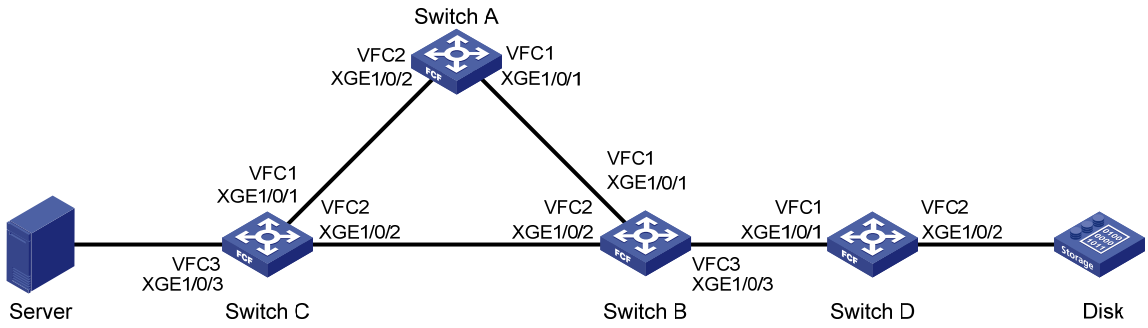
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 70, configure Switch A through Switch D to build a fabric to meet the following requirements:

- The switches in the fabric can automatically select the principal switch.
- SAN traffic can be transmitted on lossless Ethernet.
- The server can access the disk through the fabric.

Figure 70 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To implement centralized management of the network and adapt to the complex network topology, use the dynamic method to build the fabric.
- To transmit SAN traffic on lossless Ethernet:
  - Configure DCBX, PFC in auto mode, and ETS on the Ethernet interface connecting a switch to the server.
  - Configure DCBX and PFC in auto mode on the Ethernet interface connecting a switch to the disk.
  - Forcibly enable PFC on the Ethernet interfaces connecting switches.

  For more information about configuring DCBX, PFC, and ETS, see *Layer 2—LAN Switching Configuration Guide*.
- To enable the server to access the disk, configure the members in the default zone to access each other.

Configuration restrictions and guidelines

Make sure the fabric configuration function is enabled on all switches.

Configuration procedures

Configuring Switch A

1. Configure the advanced mode:

Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchA> system-view
[SwitchA] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

Save the configuration.

```
[SwitchA] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchA] quit
```

Reboot the switch.

```
<SwitchA> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

3. Configuring PFC:

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

4. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchA] fcoe-mode fcf
[SwitchA] vsan 1
[SwitchA-vsan1] domain configure enable
```

Configure the domain ID as 11 in VSAN 1.

```
[SwitchA-vsan1] domain-id 11 preferred
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchA-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchA-Vfc1] port trunk vsan 1
[SwitchA-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchA] interface vfc 2
[SwitchA-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchA-Vfc2] port trunk vsan 1
[SwitchA-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 1
[SwitchA-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchA] vsan 1
[SwitchA-vsan1] zone default-zone permit
[SwitchA-vsan1] quit
```

Configuring Switch B

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchB> system-view
   [SwitchB] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchB] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchB] quit
   ```

   # Reboot the switch.

   ```
   <SwitchB> reboot
   Start to check configuration with next startup configuration file, please
   wait.........DONE!
   Current configuration will be lost after the reboot, save current configuration?
   [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   flash:/startup.cfg exists, overwrite? [Y/N]:y
   Validating file. Please wait...
   Configuration is saved to flash successfully.
   This command will reboot the device. Continue? [Y/N]:y
   Now rebooting, please wait...
   ```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

   ```
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
   [SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
   [SwitchB-Ten-GigabitEthernet1/0/1] quit
   ```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

3. Configuring PFC:

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/3.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

4. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchB] fcoe-mode fcf
[SwitchB] vsan 1
[SwitchB-vsan1] domain configure enable
```

Configure the switch priority as 1 so that Switch B can be selected as the principal switch.

```
[SwitchB-vsan1] priority 1
[SwitchB-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchB] interface vfc 1
[SwitchB-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchB-Vfc1] port trunk vsan 1
[SwitchB-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchB] interface vfc 2
[SwitchB-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchB-Vfc2] port trunk vsan 1
[SwitchB-Vfc2] quit
```

Create interface VFC 3, and configure it to operate in E mode.

```
[SwitchB] interface vfc 3
[SwitchB-Vfc3] fc mode e
```

Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchB-Vfc3] port trunk vsan 1
[SwitchB-Vfc3] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchB] vlan 10
[SwitchB-vlan10] fcoe enable vsan 1
[SwitchB-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchB] vsan 1
[SwitchB-vsan1] zone default-zone permit
[SwitchB-vsan1] quit
```

Configuring Switch C

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchC> system-view
[SwitchC] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

   # Save the configuration.

```
[SwitchC] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
```

```
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchC] quit
```

Reboot the switch.

```
<SwitchC> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

3. Configure DCBX:

Enable LLDP globally.

```
[SwitchC] lldp global enable
```

Create an Ethernet frame header ACL numbered 4000.

```
[SwitchC] acl number 4000 name DCBX
```

Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchC-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchC-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchC-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchC] traffic classifier DCBX operator or
[SwitchC-classifier-DCBX] if-match acl 4000
[SwitchC-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchC] traffic behavior DCBX
[SwitchC-behavior-DCBX] remark dot1p 3
[SwitchC-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchC] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchC-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchC-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/3, and enable the interface to advertise DCBX TLVs.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] lldp enable
[SwitchC-Ten-GigabitEthernet1/0/3] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/3.

```
[SwitchC-Ten-GigabitEthernet1/0/3] qos apply policy DCBX outbound
```

4. Configure PFC:

Configure interface Ten-GigabitEthernet 1/0/3 to automatically negotiate with its peer to enable PFC.

```
[SwitchC-Ten-GigabitEthernet1/0/3] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

```
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

5. Configure ETS:

Configure the 802.1p-lp priority map to:

- Map 802.1p priority 3 to local precedence 1 (corresponding to queue 1).
- Map all other 802.1p priorities to local precedence 0 (corresponding to queue 0).

```
[SwitchC] qos map-table dot1p-lp
[SwitchC-maptbl-dot1p-lp] import 3 export 1
[SwitchC-maptbl-dot1p-lp] import 0 export 0
[SwitchC-maptbl-dot1p-lp] import 1 export 0
[SwitchC-maptbl-dot1p-lp] import 2 export 0
[SwitchC-maptbl-dot1p-lp] import 4 export 0
[SwitchC-maptbl-dot1p-lp] import 5 export 0
[SwitchC-maptbl-dot1p-lp] import 6 export 0
[SwitchC-maptbl-dot1p-lp] import 7 export 0
[SwitchC-maptbl-dot1p-lp] quit
```

Enable byte-count WRR on interface Ten-GigabitEthernet 1/0/3.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/3 to the SP group.

```
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr af2 group sp
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr af3 group sp
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr af4 group sp
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr ef group sp
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr cs6 group sp
[SwitchC-Ten-GigabitEthernet1/0/3] qos wrr cs7 group sp
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

6. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchC] fcoe-mode fcf
[SwitchC] vsan 1
[SwitchC-vsan1] domain configure enable
```

Configure the domain ID as 13 in VSAN 1.

```
[SwitchC-vsan1] domain-id 13 preferred
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchC-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchC] interface vfc 1
[SwitchC-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchC-Vfc1] port trunk vsan 1
[SwitchC-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchC] interface vfc 2
[SwitchC-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchC-Vfc2] port trunk vsan 1
[SwitchC-Vfc2] quit
```

Create interface VFC 3, and configure it to operate in F mode.

```
[SwitchC] interface vfc 3
[SwitchC-Vfc3] fc mode f
```

Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchC-Vfc3] port trunk vsan 1
[SwitchC-Vfc3] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchC] vlan 10
[SwitchC-vlan10] fcoe enable vsan 1
[SwitchC-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchC] vsan 1
[SwitchC-vsan1] zone default-zone permit
[SwitchC-vsan1] quit
```

Configuring Switch D

1. Configure the advanced mode:

Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchD> system-view
[SwitchD] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

Save the configuration.

```
[SwitchD] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
```

```
Save next configuration file successfully.
[SwitchD] quit
```

Reboot the switch.

```
<SwitchD> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchD] interface ten-gigabitethernet 1/0/1
[SwitchD-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchD-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchD] interface ten-gigabitethernet 1/0/2
[SwitchD-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchD-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchD-Ten-GigabitEthernet1/0/2] quit
```

3. Configure DCBX:

Enable LLDP globally.

```
[SwitchD] lldp global enable
```

Create an Ethernet frame header ACL numbered 4000.

```
[SwitchD] acl number 4000 name DCBX
```

Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchD-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchD-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchD-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchD] traffic classifier DCBX operator or
[SwitchD-classifier-DCBX] if-match acl 4000
[SwitchD-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchD] traffic behavior DCBX
[SwitchD-behavior-DCBX] remark dot1p 3
[SwitchD-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchD] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchD-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchD-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/2, and enable the interface to advertise DCBX TLVs.

```
[SwitchD] interface ten-gigabitethernet 1/0/2
[SwitchD-Ten-GigabitEthernet1/0/2] lldp enable
[SwitchD-Ten-GigabitEthernet1/0/2] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/2.

```
[SwitchD-Ten-GigabitEthernet1/0/2] qos apply policy DCBX outbound
```

4. Configure PFC:

Configure interface Ten-GigabitEthernet 1/0/2 to automatically negotiate with its peer to enable PFC.

```
[SwitchD-Ten-GigabitEthernet1/0/2] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchD-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchD-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchD-Ten-GigabitEthernet1/0/2] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

```
[SwitchD] interface ten-gigabitethernet 1/0/1
[SwitchD-Ten-GigabitEthernet1/0/1] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchD-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchD-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchD-Ten-GigabitEthernet1/0/1] quit
```

5. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchD] fcoe-mode fcf
[SwitchD] vsan 1
[SwitchD-vsan1] domain configure enable
```

Configure the domain ID as 14 in VSAN 1.

```
[SwitchD-vsan1] domain-id 14 preferred
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchD-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchD] interface vfc 1
[SwitchD-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchD-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchD-Vfc1] port trunk vsan 1
[SwitchD-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in F mode.

```
[SwitchD] interface vfc 2
[SwitchD-Vfc2] fc mode f
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchD-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchD-Vfc2] port trunk vsan 1
[SwitchD-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchD] vlan 10
[SwitchD-vlan10] fcoe enable vsan 1
[SwitchD-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchD] vsan 1
[SwitchD-vsan1] zone default-zone permit
[SwitchD-vsan1] quit
```

Verifying the configuration

Display the domain information of VSAN 1 on Switch A.

```
[SwitchA] display fc domain vsan 1
Domain Information of VSAN 1:

    Running time information:
        State: Stable
        Switch WWN: 48:33:43:2d:46:43:1A:1A
        Fabric name: 48:33:43:2d:46:43:1B:1B
        Priority: 128
        Domain ID: 11
    Configuration information:
        Domain configure: Enabled
        Domain auto-reconfigure: Disabled
        Fabric name: 48:33:43:2d:46:43:1A:1A
        Priority: 128
        Domain ID: 11 (preferred)
    Principal switch running time information:
        Priority: 1

    Path          Interface
```

```
Upstream      Vfc1
Downstream    Vfc2
```

The output shows that:

- The configuration on Switch A is completed.
- The principal switch has assigned domain ID 11 to Switch A.

Display the domain list of VSAN 1 on Switch A.

```
[SwitchA] display fc domain-list vsan 1
Domain list of VSAN 1:
  Number of domains: 4

  Domain ID      WWN
  0x01(1)        48:33:43:2d:46:43:1B:1B [Principal]
  0x0b(11)       48:33:43:2d:46:43:1A:1A [Local]
  0x0d(13)       48:33:43:2d:46:43:1C:1C
  0x0e(14)       48:33:43:2d:46:43:1D:1D
```

The output shows that Switch B has assigned domain ID 1 to itself and become the principal switch.

Configuration files

- Switch A:

```
#
 fcoe-mode fcf
#
 system-working-mode advance
#
vsan 1
 domain-id 11 preferred
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
```

```
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
```

- Switch B:

```
#
 fcoe-mode fcf
#
 system-working-mode advance
#
vsan 1
 priority 1
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
```

```
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
```

- Switch C:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 domain-id 13 preferred
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
```

```
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

- Switch D:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
```

```
 system-working-mode advance
#
vsan 1
 domain-id 14 preferred
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Vfc1
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

Example: Configuring FC static routes

Applicable product matrix

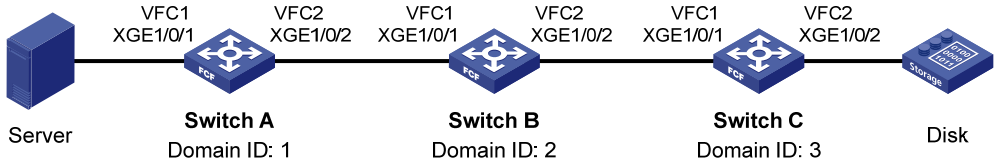
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 71, configure Switch A through Switch C to meet the following requirements:

- The switches can forward FC packets according to user-specified paths.
- SAN traffic can be transmitted on lossless Ethernet.
- The server can access the disk through the fabric.

Figure 71 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To allow FC packets to be forwarded according to user-specified paths and adapt to the simple network topology, use the static method to build the fabric and configure FC static routes.
- To allow SAN traffic to be transmitted on lossless Ethernet:
  - Configure DCBX, PFC in auto mode, and ETS on the Ethernet interface connecting a switch to a server.
  - Configure DCBX and PFC in auto mode on the Ethernet interface connecting a switch to a disk.
  - Forcibly enable PFC on the Ethernet interfaces interconnecting switches.

  For more information about configuring DCBX, PFC, and ETS, see *Layer 2—LAN Switching Configuration Guide*.
- To enable the server to access the disk, enable the members in the default zone to access each other.

Configuration restrictions and guidelines

When you configure FC static routes, follow these restrictions and guidelines:

- Make sure the domain ID for each switch in a VSAN is unique.

- Configure bidirectional FC static routes (routes for forwarding both server requests and disk responses) on all switches.

Configuration procedures

Configuring Switch A

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchA> system-view
   [SwitchA] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchA] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchA] quit
   ```

   # Reboot the switch.

   ```
   <SwitchA> reboot
   Start to check configuration with next startup configuration file, please
   wait.........DONE!
   Current configuration will be lost after the reboot, save current configuration?
   [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   flash:/startup.cfg exists, overwrite? [Y/N]:y
   Validating file. Please wait...
   Configuration is saved to flash successfully.
   This command will reboot the device. Continue? [Y/N]:y
   Now rebooting, please wait...
   ```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
   [SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

3. Configure DCBX:

Enable LLDP globally.

```
[SwitchA] lldp global enable
```

Create an Ethernet frame header ACL numbered 4000.

```
[SwitchA] acl number 4000 name DCBX
```

Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchA-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchA-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchA-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchA] traffic classifier DCBX operator or
[SwitchA-classifier-DCBX] if-match acl 4000
[SwitchA-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchA] traffic behavior DCBX
[SwitchA-behavior-DCBX] remark dot1p 3
[SwitchA-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchA] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchA-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
```

4. Configuring PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p
```

```
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

5. Configure ETS:

Configure the 802.1p-lp priority map to:

- Map 802.1p priority 3 to local precedence 1 (corresponding to queue 1).
- Map all other 802.1p priorities to local precedence 0 (corresponding to queue 0).

```
[SwitchA] qos map-table dot1p-lp
[SwitchA-maptbl-dot1p-lp] import 3 export 1
[SwitchA-maptbl-dot1p-lp] import 0 export 0
[SwitchA-maptbl-dot1p-lp] import 1 export 0
[SwitchA-maptbl-dot1p-lp] import 2 export 0
[SwitchA-maptbl-dot1p-lp] import 4 export 0
[SwitchA-maptbl-dot1p-lp] import 5 export 0
[SwitchA-maptbl-dot1p-lp] import 6 export 0
[SwitchA-maptbl-dot1p-lp] import 7 export 0
[SwitchA-maptbl-dot1p-lp] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/1 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

6. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchA] fcoe-mode fcf
[SwitchA] vsan 1
[SwitchA-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchA-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 1 in VSAN 1.

```
[SwitchA-vsan1] domain-id 1 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchA-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchA-Vfc1] port trunk vsan 1
[SwitchA-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchA] interface vfc 2
[SwitchA-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchA-Vfc2] port trunk vsan 1
[SwitchA-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 1
[SwitchA-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchA] vsan 1
[SwitchA-vsan1] zone default-zone permit
```

Configure two static routes.

```
[SwitchA-vsan1] fc route-static 020000 8 vfc 2
[SwitchA-vsan1] fc route-static 030000 8 vfc 2
[SwitchA-vsan1] quit
```

Configuring Switch B

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchB> system-view
   [SwitchB] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchB] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   ```

```
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchB] quit
```

Reboot the switch.

```
<SwitchB> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

3. Configuring PFC:

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

4. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchB] fcoe-mode fcf
[SwitchB] vsan 1
[SwitchB-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchB-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 2 in VSAN 1.

```
[SwitchB-vsan1] domain-id 2 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchB-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchB] interface vfc 1
[SwitchB-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchB-Vfc1] port trunk vsan 1
[SwitchB-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchB] interface vfc 2
[SwitchB-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchB-Vfc2] port trunk vsan 1
[SwitchB-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchB] vlan 10
[SwitchB-vlan10] fcoe enable vsan 1
[SwitchB-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchB] vsan 1
[SwitchB-vsan1] zone default-zone permit
```

Configure two static routes.

```
[SwitchB-vsan1] fc route-static 010000 8 vfc 1
[SwitchB-vsan1] fc route-static 030000 8 vfc 2
[SwitchB-vsan1] quit
```

Configuring Switch C

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchC> system-view
[SwitchC] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

   # Save the configuration.

```
[SwitchC] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchC] quit
```

   # Reboot the switch.

```
<SwitchC> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

3. Configure DCBX:

   # Enable LLDP globally.

   ```
   [SwitchC] lldp global enable
   ```

   # Create an Ethernet frame header ACL numbered 4000.

   ```
   [SwitchC] acl number 4000 name DCBX
   ```

   # Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

   ```
   [SwitchC-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
   [SwitchC-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
   [SwitchC-acl-ethernetframe-4000] quit
   ```

   # Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

   ```
   [SwitchC] traffic classifier DCBX operator or
   [SwitchC-classifier-DCBX] if-match acl 4000
   [SwitchC-classifier-DCBX] quit
   ```

   # Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

   ```
   [SwitchC] traffic behavior DCBX
   [SwitchC-behavior-DCBX] remark dot1p 3
   [SwitchC-behavior-DCBX] quit
   ```

   # Create a QoS policy named **DCBX**.

   ```
   [SwitchC] qos policy DCBX
   ```

   # Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

   ```
   [SwitchC-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
   [SwitchC-qospolicy-DCBX] quit
   ```

   # Enable LLDP on interface Ten-GigabitEthernet 1/0/2, and enable the interface to advertise DCBX TLVs.

   ```
   [SwitchC] interface ten-gigabitethernet 1/0/2
   [SwitchC-Ten-GigabitEthernet1/0/2] lldp enable
   [SwitchC-Ten-GigabitEthernet1/0/2] lldp tlv-enable dot1-tlv dcbx
   ```

   # Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/2.

   ```
   [SwitchC-Ten-GigabitEthernet1/0/2] qos apply policy DCBX outbound
   ```

4. Configure PFC:

   # Configure interface Ten-GigabitEthernet 1/0/2 to automatically negotiate with its peer to enable PFC.

   ```
   [SwitchC-Ten-GigabitEthernet1/0/2] priority-flow-control enable
   ```

   # Enable PFC for 802.1p priority 3 on the interface.

   ```
   [SwitchC-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
   ```

   # Configure the interface to trust the 802.1p priority carried in packets.

   ```
   [SwitchC-Ten-GigabitEthernet1/0/2] qos trust dot1p
   [SwitchC-Ten-GigabitEthernet1/0/2] quit
   ```

   # Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchC] interface ten-gigabitethernet 1/0/1
   [SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control enable
   ```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

5. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchC] fcoe-mode fcf
[SwitchC] vsan 1
[SwitchC-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchC-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 3 in VSAN 1.

```
[SwitchC-vsan1] domain-id 3 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchC-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchC] interface vfc 1
[SwitchC-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchC-Vfc1] port trunk vsan 1
[SwitchC-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in F mode.

```
[SwitchC] interface vfc 2
[SwitchC-Vfc2] fc mode f
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchC-Vfc2] port trunk vsan 1
[SwitchC-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchC] vlan 10
[SwitchC-vlan10] fcoe enable vsan 1
[SwitchC-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchC] vsan 1
[SwitchC-vsan1] zone default-zone permit
```

Configure two static routes.

```
[SwitchC-vsan1] fc route-static 010000 8 vfc 1
[SwitchC-vsan1] fc route-static 020000 8 vfc 1
[SwitchC-vsan1] quit
```

Verifying the configuration

Display the FC routing table of VSAN 1 on Switch A.

```
[SwitchA] display fc routing-table vsan 1
Routing Table: VSAN 1
  Destinations : 6          Routes : 6
  Destination/mask   Protocol   Preference   Cost     Interface
  0x020000/8         STATIC     10           0        Vfc2
  0x030000/8         STATIC     10           0        Vfc2
  0xfffc01/24        DIRECT     0            0        InLoop0
  0xfffffa/24        DIRECT     0            0        InLoop0
  0xfffffc/24        DIRECT     0            0        InLoop0
  0xfffffd/24        DIRECT     0            0        InLoop0
```

The output shows that the two configured static routes exist in VSAN 1 on Switch A.

Use the **fcping** command on Switch A to ping Switch C.

```
[SwitchA] fcping fcid fffc03 vsan 1
FCPING fcid 0xfffc03: 128 data bytes, press CTRL_C to break
Reply from 0xfffc03: bytes = 128 time = 23 ms
Reply from 0xfffc03: bytes = 128 time = 9 ms
Reply from 0xfffc03: bytes = 128 time = 19 ms
Reply from 0xfffc03: bytes = 128 time = 14 ms
Reply from 0xfffc03: bytes = 128 time = 25 ms

--- 0xfffc03 fcping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 9/18/25 ms
```

The output shows that Switch A can successfully ping Switch C.

Display the FC routing table of VSAN 1 on Switch B.

```
[SwitchB] display fc routing-table vsan 1
Routing Table: VSAN 1
  Destinations : 6          Routes : 6
  Destination/mask   Protocol   Preference   Cost     Interface
  0x010000/8         STATIC     10           0        Vfc1
  0x030000/8         STATIC     10           0        Vfc2
  0xfffc01/24        DIRECT     0            0        InLoop0
  0xfffffa/24        DIRECT     0            0        InLoop0
  0xfffffc/24        DIRECT     0            0        InLoop0
  0xfffffd/24        DIRECT     0            0        InLoop0
```

The output shows that the two configured static routes exist in VSAN 1 on Switch B.

Display the FC routing table of VSAN 1 on Switch C.

```
[SwitchC] display fc routing-table vsan 1
Routing Table: VSAN 1
  Destinations : 6          Routes : 6
  Destination/mask   Protocol   Preference   Cost     Interface
```

```
0x010000/8          STATIC     10           0        Vfc1
0x020000/8          STATIC     10           0        Vfc1
0xfffc01/24         DIRECT     0            0        InLoop0
0xfffffa/24         DIRECT     0            0        InLoop0
0xfffffc/24         DIRECT     0            0        InLoop0
0xfffffd/24         DIRECT     0            0        InLoop0
```

The output shows that the two configured static routes exist in VSAN 1 on Switch C.

Configuration files

- Switch A:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 1 static
 undo domain configure enable
 fc route-static 020000 8  Vfc2
 fc route-static 030000 8  Vfc2
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
```

```
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

- Switch B:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 2 static
 undo domain configure enable
 fc route-static 010000 8  Vfc1
```

```
 fc route-static 030000 8  Vfc2
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
```

- Switch C:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 3 static
 undo domain configure enable
 fc route-static 010000 8  Vfc1
 fc route-static 020000 8  Vfc1
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
```

```
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Vfc1
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

Example: Configuring FSPF

Applicable product matrix

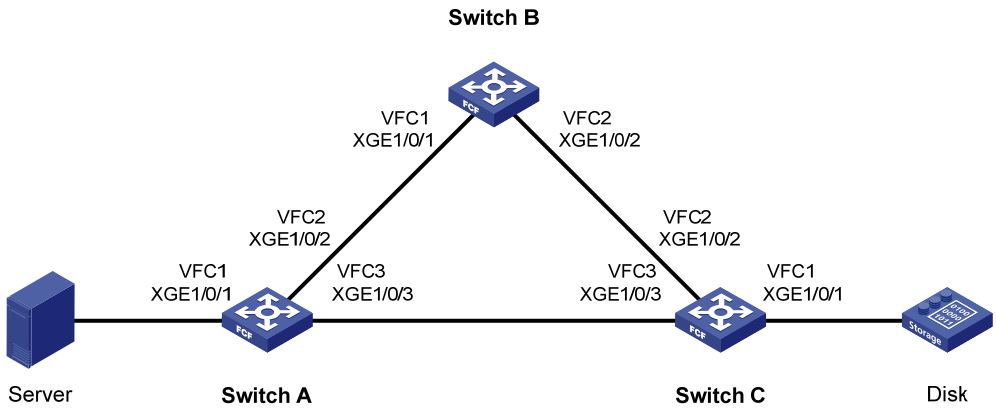
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 72, configure Switch A through Switch C to meet the following requirements:

- The switches in the fabric can forward FC packets according to FSPF routes.
- SAN traffic can be transmitted on lossless Ethernet.
- The server can access the disk through the fabric.

Figure 72 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To allow FC packets to be forwarded according to FSPF routes and adapt to the complex network topology, use the dynamic method to build the fabric and configure FSPF.
- To allow SAN traffic to be transmitted on lossless Ethernet:
  - Configure DCBX, PFC in auto mode, and ETS on the Ethernet interface connecting a switch to a server.
  - Configure DCBX and PFC in auto mode on the Ethernet interface connecting a switch to a disk.
  - Forcibly enable PFC on the Ethernet interfaces interconnecting switches.

  For more information about configuring DCBX, PFC, and ETS, see *Layer 2—LAN Switching Configuration Guide*.
- To enable the server to access the disk, enable the members in the default zone to access each other.

Configuration restrictions and guidelines

To use FSPF, enable FSPF on VFC interfaces in E mode and in the VSAN to which these interfaces belong.

Configuration procedures

Configuring Switch A

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchA> system-view
   [SwitchA] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchA] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchA] quit
   ```

   # Reboot the switch.

   ```
   <SwitchA> reboot
   Start to check configuration with next startup configuration file, please
   wait.........DONE!
   Current configuration will be lost after the reboot, save current configuration?
   [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   flash:/startup.cfg exists, overwrite? [Y/N]:y
   Validating file. Please wait...
   Configuration is saved to flash successfully.
   This command will reboot the device. Continue? [Y/N]:y
   Now rebooting, please wait...
   ```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
   ```

```
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

3. Configure DCBX:

Enable LLDP globally.

```
[SwitchA] lldp global enable
```

Create an Ethernet frame header ACL numbered 4000.

```
[SwitchA] acl number 4000 name DCBX
```

Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchA-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchA-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchA-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchA] traffic classifier DCBX operator or
[SwitchA-classifier-DCBX] if-match acl 4000
[SwitchA-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchA] traffic behavior DCBX
[SwitchA-behavior-DCBX] remark dot1p 3
[SwitchA-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchA] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchA-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
```

4. Configuring PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/3.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

5. Configure ETS:

Configure the 802.1p-lp priority map to:

- Map 802.1p priority 3 to local precedence 1 (corresponding to queue 1).
- Map all other 802.1p priorities to local precedence 0 (corresponding to queue 0).

```
[SwitchA] qos map-table dot1p-lp
[SwitchA-maptbl-dot1p-lp] import 3 export 1
[SwitchA-maptbl-dot1p-lp] import 0 export 0
[SwitchA-maptbl-dot1p-lp] import 1 export 0
[SwitchA-maptbl-dot1p-lp] import 2 export 0
[SwitchA-maptbl-dot1p-lp] import 4 export 0
[SwitchA-maptbl-dot1p-lp] import 5 export 0
[SwitchA-maptbl-dot1p-lp] import 6 export 0
[SwitchA-maptbl-dot1p-lp] import 7 export 0
[SwitchA-maptbl-dot1p-lp] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/1 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

6. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchA] fcoe-mode fcf
[SwitchA] vsan 1
[SwitchA-vsan1] domain configure enable
```

Configure the switch priority as 1 so that Switch A can be selected as the principal switch.

```
[SwitchA-vsan1] priority 1
[SwitchA-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchA-Vfc1] port trunk vsan 1
[SwitchA-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchA] interface vfc 2
[SwitchA-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchA-Vfc2] port trunk vsan 1
[SwitchA-Vfc2] quit
```

Create interface VFC 3, and configure it to operate in E mode.

```
[SwitchA] interface vfc 3
[SwitchA-Vfc3] fc mode e
```

Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchA-Vfc3] port trunk vsan 1
[SwitchA-Vfc3] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 1
[SwitchA-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchA] vsan 1
[SwitchA-vsan1] zone default-zone permit
```

Enable FSPF for VSAN 1.

```
[SwitchA-vsan1] fspf enable
[SwitchA-vsan1] quit
```

Enable FSPF on VFC 2.

```
[SwitchA] interface vfc 2
[SwitchA-Vfc2] undo fspf silent vsan 1
[SwitchA-Vfc2] quit
```

Enable FSPF on VFC 3.

```
[SwitchA] interface vfc 3
[SwitchA-Vfc3] undo fspf silent vsan 1
[SwitchA-Vfc3] quit
```

Configuring Switch B

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchB> system-view
   [SwitchB] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchB] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchB] quit
   ```

   # Reboot the switch.

   ```
   <SwitchB> reboot
   Start to check configuration with next startup configuration file, please
   wait.........DONE!
   Current configuration will be lost after the reboot, save current configuration?
   [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   flash:/startup.cfg exists, overwrite? [Y/N]:y
   Validating file. Please wait...
   Configuration is saved to flash successfully.
   This command will reboot the device. Continue? [Y/N]:y
   Now rebooting, please wait...
   ```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

3. Configuring PFC:

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/1.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

4. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchB] fcoe-mode fcf
[SwitchB] vsan 1
[SwitchB-vsan1] domain configure enable
```

Configure the domain ID as 2 in VSAN 1.

```
[SwitchB-vsan1] domain-id 2 preferred
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchB-vsan1] quit
```

Create interface VFC 1, and configure it to operate in E mode.

```
[SwitchB] interface vfc 1
[SwitchB-Vfc1] fc mode e
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchB-Vfc1] port trunk vsan 1
[SwitchB-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchB] interface vfc 2
[SwitchB-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchB-Vfc2] port trunk vsan 1
[SwitchB-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchB] vlan 10
[SwitchB-vlan10] fcoe enable vsan 1
[SwitchB-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchB] vsan 1
[SwitchB-vsan1] zone default-zone permit
```

Enable FSPF for VSAN 1.

```
[SwitchB-vsan1] fspf enable
[SwitchB-vsan1] quit
```

Enable FSPF on VFC 1.

```
[SwitchB] interface vfc 1
[SwitchB-Vfc1] undo fspf silent vsan 1
[SwitchB-Vfc1] quit
```

Enable FSPF on VFC 2.

```
[SwitchB] interface vfc 2
[SwitchB-Vfc2] undo fspf silent vsan 1
[SwitchB-Vfc2] quit
```

Configuring Switch C

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchC> system-view
   [SwitchC] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchC] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   ```

```
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchC] quit
```

Reboot the switch.

```
<SwitchC> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

3. Configure DCBX:

Enable LLDP globally.

```
[SwitchC] lldp global enable
```

Create an Ethernet frame header ACL numbered 4000.

```
[SwitchC] acl number 4000 name DCBX
```

Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchC-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchC-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchC-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchC] traffic classifier DCBX operator or
[SwitchC-classifier-DCBX] if-match acl 4000
[SwitchC-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchC] traffic behavior DCBX
[SwitchC-behavior-DCBX] remark dot1p 3
[SwitchC-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchC] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchC-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchC-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchC-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchC-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
```

4. Configure PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/2.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/3.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchC-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchC-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

5. Configure FCoE:

Configure the switch to operate in FCF mode, and enable the fabric configuration function in VSAN 1. By default, the fabric configuration function is enabled.

```
[SwitchC] fcoe-mode fcf
[SwitchC] vsan 1
[SwitchC-vsan1] domain configure enable
```

Configure the domain ID as 3 in VSAN 1.

```
[SwitchC-vsan1] domain-id 3 preferred
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchC-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchC] interface vfc 1
[SwitchC-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchC-Vfc1] port trunk vsan 1
[SwitchC-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in E mode.

```
[SwitchC] interface vfc 2
[SwitchC-Vfc2] fc mode e
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchC-Vfc2] port trunk vsan 1
[SwitchC-Vfc2] quit
```

Create interface VFC 3, and configure it to operate in E mode.

```
[SwitchC] interface vfc 3
[SwitchC-Vfc3] fc mode e
```

Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchC-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchC-Vfc3] port trunk vsan 1
[SwitchC-Vfc3] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchC] vlan 10
[SwitchC-vlan10] fcoe enable vsan 1
[SwitchC-vlan10] quit
```

Permit the members in the default zone of VSAN 1 to access each other.

```
[SwitchC] vsan 1
[SwitchC-vsan1] zone default-zone permit
```

Enable FSPF for VSAN 1.

```
[SwitchC-vsan1] fspf enable
[SwitchC-vsan1] quit
```

Enable FSPF on VFC 2.

```
[SwitchC] interface vfc 2
[SwitchC-Vfc2] undo fspf silent vsan 1
[SwitchC-Vfc2] quit
```

Enable FSPF on VFC 3.

```
[SwitchC] interface vfc 3
[SwitchC-Vfc3] undo fspf silent vsan 1
[SwitchC-Vfc3] quit
```

Verifying the configuration

Verifying the configuration on Switch A

Display the FSPF neighbor information for VSAN 1.

```
[SwitchA] display fspf neighbor
FSPF neighbor information of VSAN 1(01):
  Interface    NbrDomain    IfIndex    NbrIfIndex    Dead Time    State
  Vfc2         2            0x68       0x68          00:01:06     Full
  Vfc3         3            0x69       0x69          00:01:06     Full
```

The output shows that Switch A has two neighbors in VSAN 1 (Switch B and Switch C).

Display the FC routing table of VSAN 1.

```
[SwitchA] display fc routing-table vsan 1
Routing Table: VSAN 1
  Destinations : 6          Routes : 6
  Destination/mask    Protocol    Preference    Cost      Interface
  0x020000/8          FSPF        20            100       Vfc2
  0x030000/8          FSPF        20            100       Vfc3
  0xfffc01/24         DIRECT      0             0         InLoop0
  0xfffffa/24         DIRECT      0             0         InLoop0
  0xfffffc/24         DIRECT      0             0         InLoop0
  0xfffffd/24         DIRECT      0             0         InLoop0
```

The output shows that two FSPF routes exist in VSAN 1.

Use the **fcping** command on Switch A to ping Switch C.

```
[SwitchA] fcping fcid fffc03 vsan 1
FCPING fcid 0xfffc03: 128 data bytes, press CTRL_C to break
Reply from 0xfffc03: bytes = 128 time = 23 ms
Reply from 0xfffc03: bytes = 128 time = 9 ms
Reply from 0xfffc03: bytes = 128 time = 19 ms
Reply from 0xfffc03: bytes = 128 time = 14 ms
Reply from 0xfffc03: bytes = 128 time = 25 ms

--- 0xfffc03 fcping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
```

```
round-trip min/avg/max = 9/18/25 ms
```

The output shows that Switch A can successfully ping Switch C.

Verifying the configuration on Switch B

Display the FC routing table of VSAN 1.

```
[SwitchB] display fc routing-table vsan 1
Routing Table: VSAN 1
  Destinations : 6          Routes : 6
  Destination/mask    Protocol    Preference    Cost      Interface
  0x010000/8          FSPF        20            100       Vfc1
  0x030000/8          FSPF        20            100       Vfc2
  0xfffc01/24         DIRECT      0             0         InLoop0
  0xfffffa/24         DIRECT      0             0         InLoop0
  0xfffffc/24         DIRECT      0             0         InLoop0
  0xfffffd/24         DIRECT      0             0         InLoop0
```

The output shows that two FSPF routes exist in VSAN 1.

Verifying the configuration on Switch C

Display the FC routing table of VSAN 1.

```
[SwitchC] display fc routing-table vsan 1
Routing Table: VSAN 1
  Destinations : 6          Routes : 6
  Destination/mask    Protocol    Preference    Cost      Interface
  0x010000/8          FSPF        20            100       Vfc3
  0x020000/8          FSPF        20            100       Vfc2
  0xfffc01/24         DIRECT      0             0         InLoop0
  0xfffffa/24         DIRECT      0             0         InLoop0
  0xfffffc/24         DIRECT      0             0         InLoop0
  0xfffffd/24         DIRECT      0             0         InLoop0
```

The output shows that two FSPF routes exist in VSAN 1.

Configuration files

- Switch A:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 priority 1
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
```

```
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
```

```
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

- Switch B:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 domain-id 2 preferred
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
```

```
interface Vfc1
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
```

- Switch C:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 domain-id 3 preferred
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
```

```
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

Example: Configuring FC zones

Applicable product matrix

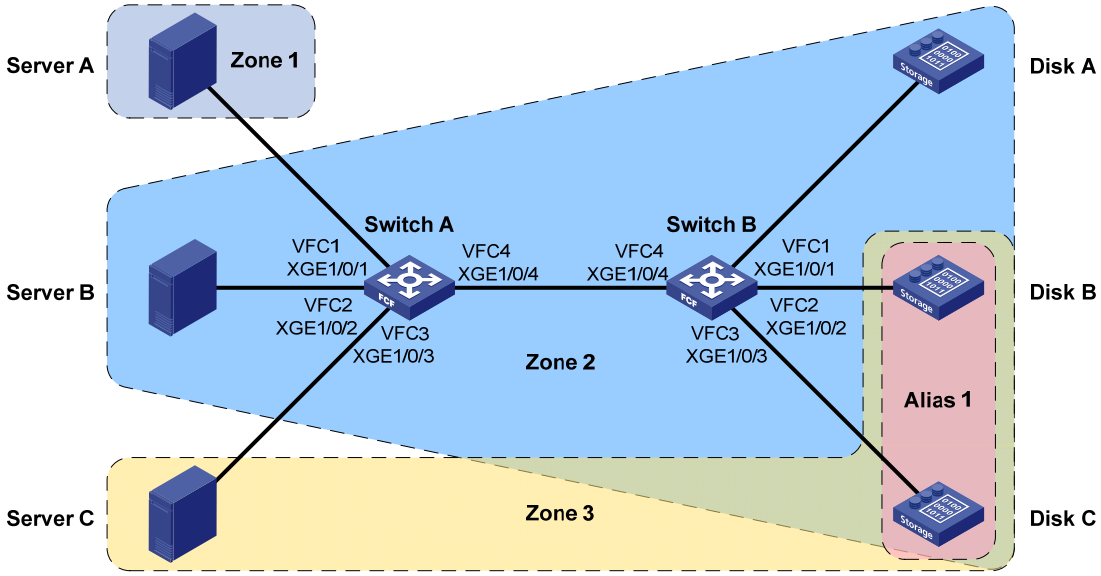
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 73, configure Switch A and Switch B to meet the following requirements:

- SAN traffic can be transmitted on lossless Ethernet.
- Server A does not access any disk but might need to subsequently.
- Server B can access Disks A, B, and C.
- Server C can access Disks B and C.
- Servers cannot access each other.

Figure 73 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To adapt to the simple network topology, use the static method to build a fabric.
- To allow SAN traffic to be transmitted on lossless Ethernet:
  - Configure DCBX, PFC in auto mode, and ETS on the Ethernet interface connecting a switch to a server.
  - Configure DCBX and PFC in auto mode on the Ethernet interface connecting a switch to a disk.
  - Forcibly enable PFC on the Ethernet interfaces interconnecting switches.

  For more information about configuring DCBX, PFC, and ETS, see *Layer 2—LAN Switching Configuration Guide*.
- To implement access control over the servers and disks (N_Ports), assign these N_Ports to three zones:
  - Zone1 (containing Server A).
  - Zone2 (containing Server B, Disk A, Disk B, and Disk C).
  - Zone3 (containing Server C, Disk B, and Disk C).
- To simplify configuration, create a zone alias Alias1 to contain Disk B and Disk C, which belong to both Zone2 and Zone3.
- For all switches in the fabric to implement consistent access control over the N_Ports, specify the active zone set on a switch and distribute it throughout the fabric.
- To distribute the active zone set throughout the fabric, configure the zone distribution and merge types. Because there is only one zone set and all N_Ports are in that zone set, you can configure the zone distribution and merge types as complete or incomplete distribution and merge.

Configuration procedures

Configuring Switch A

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchA> system-view
[SwitchA] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

   # Save the configuration.

```
[SwitchA] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchA] quit
```

   # Reboot the switch.

```
<SwitchA> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
```

```
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Assign interface Ten-GigabitEthernet 1/0/4 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/4] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

3. Configure DCBX:

Enable LLDP globally.

```
[SwitchA] lldp global enable
```

Create an Ethernet frame header ACL numbered 4000.

```
[SwitchA] acl number 4000 name DCBX
```

Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchA-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchA-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchA-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchA] traffic classifier DCBX operator or
[SwitchA-classifier-DCBX] if-match acl 4000
[SwitchA-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchA] traffic behavior DCBX
[SwitchA-behavior-DCBX] remark dot1p 3
[SwitchA-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchA] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchA-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
```

```
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/2, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/2] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/2.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy DCBX outbound
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/3, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/3] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/3.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos apply policy DCBX outbound
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

4. Configuring PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Configure interface Ten-GigabitEthernet 1/0/2 to automatically negotiate with its peer to enable PFC.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Configure interface Ten-GigabitEthernet 1/0/3 to automatically negotiate with its peer to enable PFC.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/4.

```
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/4] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/4] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

5. Configure ETS:

Configure the 802.1p-lp priority map to:

- Map 802.1p priority 3 to local precedence 1 (corresponding to queue 1).
- Map all other 802.1p priorities to local precedence 0 (corresponding to queue 0).

```
[SwitchA] qos map-table dot1p-lp
[SwitchA-maptbl-dot1p-lp] import 3 export 1
[SwitchA-maptbl-dot1p-lp] import 0 export 0
[SwitchA-maptbl-dot1p-lp] import 1 export 0
[SwitchA-maptbl-dot1p-lp] import 2 export 0
[SwitchA-maptbl-dot1p-lp] import 4 export 0
[SwitchA-maptbl-dot1p-lp] import 5 export 0
[SwitchA-maptbl-dot1p-lp] import 6 export 0
[SwitchA-maptbl-dot1p-lp] import 7 export 0
[SwitchA-maptbl-dot1p-lp] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/1. Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic and the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/1 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/2 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/3.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/3 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/3] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

6. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchA] fcoe-mode fcf
[SwitchA] vsan 1
[SwitchA-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchA-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 1 in VSAN 1.

```
[SwitchA-vsan1] domain-id 1 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchA-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchA-Vfc1] port trunk vsan 1
[SwitchA-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in F mode.

```
[SwitchA] interface vfc 2
```

```
[SwitchA-Vfc2] fc mode f
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchA-Vfc2] port trunk vsan 1
[SwitchA-Vfc2] quit
```

Create interface VFC 3, and configure it to operate in F mode.

```
[SwitchA] interface vfc 3
[SwitchA-Vfc3] fc mode f
```

Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchA-Vfc3] port trunk vsan 1
[SwitchA-Vfc3] quit
```

Create interface VFC 4, and configure it to operate in E mode.

```
[SwitchA] interface vfc 4
[SwitchA-Vfc4] fc mode e
```

Bind interface VFC 4 to interface Ten-GigabitEthernet 1/0/4, and assign it to VSAN 1 as a trunk port.

```
[SwitchA-Vfc4] bind interface ten-gigabitethernet 1/0/4
[SwitchA-Vfc4] port trunk vsan 1
[SwitchA-Vfc4] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 1
[SwitchA-vlan10] quit
```

Configuring Switch B

1. Configure the advanced mode:

Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchB> system-view
[SwitchB] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

Save the configuration.

```
[SwitchB] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchB] quit
```

Reboot the switch.

```
<SwitchB> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/4 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/4
[SwitchB-Ten-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/4] port trunk permit vlan 10
[SwitchB-Ten-GigabitEthernet1/0/4] quit
```

3. Configure DCBX:

   # Enable LLDP globally.

```
[SwitchB] lldp global enable
```

   # Create an Ethernet frame header ACL numbered 4000.

```
[SwitchB] acl number 4000 name DCBX
```

   # Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchB-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchB-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchB-acl-ethernetframe-4000] quit
```

Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchB] traffic classifier DCBX operator or
[SwitchB-classifier-DCBX] if-match acl 4000
[SwitchB-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchB] traffic behavior DCBX
[SwitchB-behavior-DCBX] remark dot1p 3
[SwitchB-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchB] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchB-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchB-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchB-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/2, and enable the interface to advertise DCBX TLVs.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] lldp enable
[SwitchB-Ten-GigabitEthernet1/0/2] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/2.

```
[SwitchB-Ten-GigabitEthernet1/0/2] qos apply policy DCBX outbound
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/3, and enable the interface to advertise DCBX TLVs.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] lldp enable
[SwitchB-Ten-GigabitEthernet1/0/3] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/3.

```
[SwitchB-Ten-GigabitEthernet1/0/3] qos apply policy DCBX outbound
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

4. Configuring PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Configure interface Ten-GigabitEthernet 1/0/2 to automatically negotiate with its peer to enable PFC.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Configure interface Ten-GigabitEthernet 1/0/3 to automatically negotiate with its peer to enable PFC.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/4.

```
[SwitchB] interface ten-gigabitethernet 1/0/4
[SwitchB-Ten-GigabitEthernet1/0/4] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/4] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/4] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/4] quit
```

5. Configure FCoE:

Configure the switch to operate in FCF mode, and disable the fabric configuration function in VSAN 1.

```
[SwitchB] fcoe-mode fcf
[SwitchB] vsan 1
[SwitchB-vsan1] undo domain configure enable
```

Configure a fabric name in VSAN 1.

```
[SwitchB-vsan1] fabric-name 11:11:11:11:11:11:11:11
```

Configure the domain ID as 2 in VSAN 1.

```
[SwitchB-vsan1] domain-id 2 static
Non-disruptive reconfiguration or isolating the switch may be performed. Continue?
[Y/N]:y
[SwitchB-vsan1] quit
```

Create interface VFC 1, and configure it to operate in F mode.

```
[SwitchB] interface vfc 1
```

```
[SwitchB-Vfc1] fc mode f
```

Bind interface VFC 1 to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchB-Vfc1] port trunk vsan 1
[SwitchB-Vfc1] quit
```

Create interface VFC 2, and configure it to operate in F mode.

```
[SwitchB] interface vfc 2
[SwitchB-Vfc2] fc mode f
```

Bind interface VFC 2 to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchB-Vfc2] port trunk vsan 1
[SwitchB-Vfc2] quit
```

Create interface VFC 3, and configure it to operate in F mode.

```
[SwitchB] interface vfc 3
[SwitchB-Vfc3] fc mode f
```

Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchB-Vfc3] port trunk vsan 1
[SwitchB-Vfc3] quit
```

Create interface VFC 4, and configure it to operate in E mode.

```
[SwitchB] interface vfc 4
[SwitchB-Vfc4] fc mode e
```

Bind interface VFC 4 to interface Ten-GigabitEthernet 1/0/4, and assign it to VSAN 1 as a trunk port.

```
[SwitchB-Vfc4] bind interface ten-gigabitethernet 1/0/4
[SwitchB-Vfc4] port trunk vsan 1
[SwitchB-Vfc4] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchB] vlan 10
[SwitchB-vlan10] fcoe enable vsan 1
[SwitchB-vlan10] quit
```

Configuring FC zones

You only need to configure FC zones on one switch. The following example uses Switch A.

NOTE:

You can use the **display fc login** command on Switch A and Switch B to identify the FC addresses assigned the nodes. In this example, Switch A assigned FC addresses 0x010000, 0x010001, and 0x010002 to Server A, Server B, and Server C, respectively. Switch B assigned FC addresses 0x020000, 0x020001, and 0x020002 to Disk A, Disk B, and Disk C, respectively.

Create a zone alias named **Alias1**, and specify FC addresses 020001 and 020002 as its members.

```
[SwitchA] vsan 1
[SwitchA-vsan1] zone-alias name Alias1
```

```
[SwitchA-vsan1-zone-alias-Alias1] member fcid 020001
[SwitchA-vsan1-zone-alias-Alias1] member fcid 020002
[SwitchA-vsan1-zone-alias-Alias1] quit
```

Create a zone named **Zone1**, and specify FC address 010000 as its member.

```
[SwitchA-vsan1] zone name Zone1
[SwitchA-vsan1-zone-Zone1] member fcid 010000
[SwitchA-vsan1-zone-Zone1] quit
```

Create a zone named **Zone2**, and specify FC addresses 010001 and 020000 and zone alias **Alias1** as its members.

```
[SwitchA-vsan1] zone name Zone2
[SwitchA-vsan1-zone-Zone2] member fcid 010001
[SwitchA-vsan1-zone-Zone2] member fcid 020000
[SwitchA-vsan1-zone-Zone2] member zone-alias Alias1
[SwitchA-vsan1-zone-Zone2] quit
```

Create a zone named **Zone3**, and specify FC address 010002 and zone alias **Alias1** as its members.

```
[SwitchA-vsan1] zone name Zone3
[SwitchA-vsan1-zone-Zone3] member fcid 010002
[SwitchA-vsan1-zone-Zone3] member zone-alias Alias1
[SwitchA-vsan1-zone-Zone3] quit
```

Create a zone set named **Zoneset1**, and specify zones **Zone1**, **Zone2**, and **Zone3** as its members.

```
[SwitchA-vsan1] zoneset name Zoneset1
[SwitchA-vsan1-zoneset-Zoneset1] member Zone1
[SwitchA-vsan1-zoneset-Zoneset1] member Zone2
[SwitchA-vsan1-zoneset-Zoneset1] member Zone3
[SwitchA-vsan1-zoneset-Zoneset1] quit
```

Configure zone distribution and merge types as **complete distribution** and **complete merge**.

```
[SwitchA-vsan1] zoneset distribute full
```

Activate the zone set **Zoneset1** as the active zone set, and distribute it to the entire fabric.

```
[SwitchA-vsan1] zoneset activate name Zoneset1
```

Verifying the configuration

The following verifies the configuration on Switch B.

Display the zone set information of VSAN 1.

```
[SwitchB] display zoneset vsan 1
VSAN 1:
  zoneset name Zoneset1
    zone name Zone1
      fcid 0x010000
    zone name Zone2
      fcid 0x010001
      fcid 0x020000
      zone-alias name Alias1
        fcid 0x020001
        fcid 0x020002
    zone name Zone3
```

```
    fcid 0x010002
    zone-alias name Alias1
      fcid 0x020001
      fcid 0x020002
```

The output shows that all zone configurations on Switch A have been synchronized to Switch B.

Display information about the zone **Zone2** in VSAN 1.

```
[SwitchB] display zone name Zone2 vsan 1
VSAN 1:
  zone name Zone2
    fcid 0x010001
    fcid 0x020000
    zone-alias name Alias1
      fcid 0x020001
      fcid 0x020002
```

Display information about all zone aliases.

```
[SwitchB] display zone-alias
VSAN 1:
  zone-alias name Alias1
    fcid 0x020001
    fcid 0x020002
```

Display the zones and zone aliases to which FC address 020002 belongs.

```
[SwitchB] display zone member fcid 020002
fcid 0x020002
  VSAN 1:
    zone-alias Alias1
      zone Zone2
      zone Zone3
```

Display information about the active zone set in VSAN 1.

```
[SwitchB] display zoneset active vsan 1
VSAN 1:
  zoneset name Zoneset1
    zone name Zone1
      *fcid 0x010000
    zone name Zone2
      *fcid 0x010001
      *fcid 0x020000
      *fcid 0x020001
      *fcid 0x020002
    zone name Zone3
      *fcid 0x010002
      *fcid 0x020001
      *fcid 0x020002
```

Configuration files

- Switch A:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 1 static
 undo domain configure enable
 zone-alias name Alias1
  member fcid 020001
  member fcid 020002
 zone name Zone1
  member fcid 010000
 zone name Zone2
  member zone-alias Alias1
  member fcid 010001
  member fcid 020000
 zone name Zone3
  member zone-alias Alias1
  member fcid 010002
 zoneset name Zoneset1
  member Zone1
  member Zone2
  member Zone3
 zoneset distribute full
 zoneset activate name Zoneset1
#
vlan 10
 fcoe enable vsan 1
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
```

```
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
```

```
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
interface Vfc4
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/4
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

- Switch B:

```
#
 fcoe-mode fcf
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 fabric-name 11:11:11:11:11:11:11:11
 domain-id 2 static
 undo domain configure enable
#
vlan 10
 fcoe enable vsan 1
#
traffic classifier DCBX operator or
```

```
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 port trunk vsan 1
```

```
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
interface Vfc4
 fc mode e
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/4
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

Example: Configuring NPV

Applicable product matrix

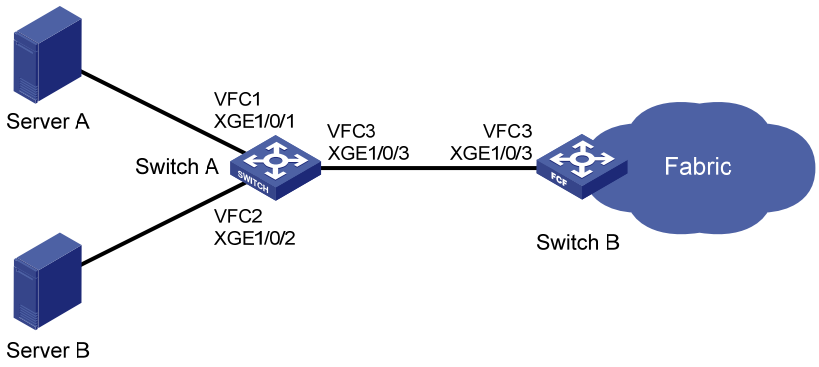
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 74, configure Switch A (edge switch) and Switch B (core switch) to meet the following requirements:

- SAN traffic can be transmitted on lossless Ethernet.
- The FC SAN can be expanded to accommodate more than 239 edge switches in a fabric.
- Server A and Server B can access the fabric through Switch A.

Figure 74 Network diagram



Requirements analysis

To meet the network requirements, perform the following tasks:

- To allow SAN traffic to be transmitted on lossless Ethernet:
  - Configure DCBX, PFC in auto mode, and ETS on the Ethernet interface connecting a switch to the server.
  - Configure DCBX and PFC in auto mode on the Ethernet interface connecting a switch to the disk.
  - Forcibly enable PFC on the Ethernet interfaces interconnecting switches.

  For more information about configuring DCBX, PFC, and ETS, see *Layer 2—LAN Switching Configuration Guide*.
- To expand the network, add edge switches between nodes and the core switch and configure the edge switches to operate in NPV mode.
- To enable the server to access the fabric, permit the members in the default zone to access each other.

Configuration restrictions and guidelines

On the NPV switch, configure the interfaces connecting to the nodes to operate in F mode, and configure the interface connecting to the core switch to operate in NP mode.

Configuration procedures

Configuring Switch A

1. Configure the advanced mode:

   # Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

   ```
   <SwitchA> system-view
   [SwitchA] system-working-mode advance
   Do you want to change the system working mode? [Y/N]:y
   The system working mode is changed, please save the configuration and reboot the
    system to make it effective.
   ```

   # Save the configuration.

   ```
   [SwitchA] save
   The current configuration will be written to the device. Are you sure? [Y/N]:y
   Please input the file name(*.cfg)[flash:/startup.cfg]
   (To leave the existing filename unchanged, press the enter key):
   Validating file. Please wait...
   Saved the current configuration to mainboard device successfully.
   Slot 1:
   Save next configuration file successfully.
   [SwitchA] quit
   ```

   # Reboot the switch.

   ```
   <SwitchA> reboot
   ```

```
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

   # Create VLAN 10.

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

   # Assign interface Ten-GigabitEthernet 1/0/1 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/2 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

   # Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

3. Configure DCBX:

   # Enable LLDP globally.

```
[SwitchA] lldp global enable
```

   # Create an Ethernet frame header ACL numbered 4000.

```
[SwitchA] acl number 4000 name DCBX
```

   # Configure two rules in the ACL to match FCoE frames (protocol type 0x8906) and FIP frames (protocol type 0x8914).

```
[SwitchA-acl-ethernetframe-4000] rule 0 permit type 8906 ffff
[SwitchA-acl-ethernetframe-4000] rule 5 permit type 8914 ffff
[SwitchA-acl-ethernetframe-4000] quit
```

   # Create a class named **DCBX** with the operator as OR, and specify ACL 4000 as the match criterion.

```
[SwitchA] traffic classifier DCBX operator or
[SwitchA-classifier-DCBX] if-match acl 4000
[SwitchA-classifier-DCBX] quit
```

Create a behavior named **DCBX**, and configure the action of marking packets with 802.1p priority 3.

```
[SwitchA] traffic behavior DCBX
[SwitchA-behavior-DCBX] remark dot1p 3
[SwitchA-behavior-DCBX] quit
```

Create a QoS policy named **DCBX**.

```
[SwitchA] qos policy DCBX
```

Associate the class **DCBX** with the behavior **DCBX** in the QoS policy, and specify that the class-behavior association applies only to DCBX.

```
[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx
[SwitchA-qospolicy-DCBX] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/1, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable LLDP on interface Ten-GigabitEthernet 1/0/2, and enable the interface to advertise DCBX TLVs.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/2] lldp tlv-enable dot1-tlv dcbx
```

Apply the QoS policy **DCBX** to the outbound direction of Ten-GigabitEthernet 1/0/2.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy DCBX outbound
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

4. Configuring PFC:

Configure interface Ten-GigabitEthernet 1/0/1 to automatically negotiate with its peer to enable PFC.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Configure interface Ten-GigabitEthernet 1/0/2 to automatically negotiate with its peer to enable PFC.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control auto
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/3.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchA-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

5. Configure ETS:

Configure the 802.1p-lp priority map to:

- Map 802.1p priority 3 to local precedence 1 (corresponding to queue 1).
- Map all other 802.1p priorities to local precedence 0 (corresponding to queue 0).

```
[SwitchA] qos map-table dot1p-lp
[SwitchA-maptbl-dot1p-lp] import 3 export 1
[SwitchA-maptbl-dot1p-lp] import 0 export 0
[SwitchA-maptbl-dot1p-lp] import 1 export 0
[SwitchA-maptbl-dot1p-lp] import 2 export 0
[SwitchA-maptbl-dot1p-lp] import 4 export 0
[SwitchA-maptbl-dot1p-lp] import 5 export 0
[SwitchA-maptbl-dot1p-lp] import 6 export 0
[SwitchA-maptbl-dot1p-lp] import 7 export 0
[SwitchA-maptbl-dot1p-lp] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/1 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr byte-count
```

Assign 50% of the interface bandwidth to queue 1 (**af1**) for FCoE traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af1 group 1 byte-count 1
```

Assign the other 50% to queue 0 (**be**) for standard LAN traffic.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr be group 1 byte-count 1
```

Assign all other queues on Ten-GigabitEthernet 1/0/2 to the SP group.

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

6. Configure FCoE:

Configure the switch to operate in NPV mode, and enter the view of VSAN 1.

```
[SwitchA] fcoe-mode npv
[SwitchA] vsan 1
[SwitchA-vsan1] quit
```

Create interface VFC 1, bind it to interface Ten-GigabitEthernet 1/0/1, and assign it to VSAN 1 as a trunk port.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1
[SwitchA-Vfc1] port trunk vsan 1
[SwitchA-Vfc1] quit
```

Create interface VFC 2, bind it to interface Ten-GigabitEthernet 1/0/2, and assign it to VSAN 1 as a trunk port.

```
[SwitchA] interface vfc 2
[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2
[SwitchA-Vfc2] port trunk vsan 1
[SwitchA-Vfc2] quit
```

Create interface VFC 3, bind it to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

```
[SwitchA] interface vfc 3
[SwitchA-Vfc3] bind interface ten-gigabitethernet 1/0/3
[SwitchA-Vfc3] port trunk vsan 1
```

Configure the uplink interface VFC 3.

```
[SwitchA-Vfc3] fc mode np
[SwitchA-Vfc3] quit
```

Configure the downlink interfaces VFC 1 and VFC 2.

```
[SwitchA] interface vfc 1
[SwitchA-Vfc1] fc mode f
[SwitchA-Vfc1] quit
[SwitchA] interface vfc 2
[SwitchA-Vfc2] fc mode f
[SwitchA-Vfc2] quit
```

Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 1
[SwitchA-vlan10] quit
```

Configuring Switch B

1. Configure the advanced mode:

Configure the switch to operate in advanced mode. (Skip this step if the switch is already operating in advanced mode.)

```
<SwitchB> system-view
[SwitchB] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
The system working mode is changed, please save the configuration and reboot the
 system to make it effective.
```

Save the configuration.

```
[SwitchB] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
[SwitchB] quit
```

Reboot the switch.

```
<SwitchB> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to flash successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

2. Configure a VLAN and Ethernet interfaces:

Create VLAN 10.

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

Assign interface Ten-GigabitEthernet 1/0/3 to VLAN 10 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10
```

3. Configuring PFC:

Forcibly enable PFC on interface Ten-GigabitEthernet 1/0/3.

```
[SwitchB-Ten-GigabitEthernet1/0/3] priority-flow-control enable
```

Enable PFC for 802.1p priority 3 on the interface.

```
[SwitchB-Ten-GigabitEthernet1/0/3] priority-flow-control no-drop dot1p 3
```

Configure the interface to trust the 802.1p priority carried in packets.

```
[SwitchB-Ten-GigabitEthernet1/0/3] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

4. Configure FCoE:

   # Configure the switch to operate in FCF mode, and enter the view of VSAN 1.

   ```
   [SwitchB] fcoe-mode fcf
   [SwitchB] vsan 1
   [SwitchB-vsan1] quit
   ```

   # Create interface VFC 3, and configure it to operate in F mode.

   ```
   [SwitchB] interface vfc 3
   [SwitchB-Vfc3] fc mode f
   ```

   # Bind interface VFC 3 to interface Ten-GigabitEthernet 1/0/3, and assign it to VSAN 1 as a trunk port.

   ```
   [SwitchB-Vfc3] bind interface ten-gigabitethernet 1/0/3
   [SwitchB-Vfc3] port trunk vsan 1
   [SwitchB-Vfc3] quit
   ```

   # Enable FCoE for VLAN 10 and map VLAN 10 to VSAN 1.

   ```
   [SwitchB] vlan 10
   [SwitchB-vlan10] fcoe enable vsan 1
   [SwitchB-vlan10] quit
   ```

   # Permit the members in the default zone of VSAN 1 to access each other.

   ```
   [SwitchC] vsan 1
   [SwitchC-vsan1] zone default-zone permit
   [SwitchC-vsan1] quit
   ```

Verifying the configuration

Display the nodes on downlink interfaces and the mapped uplink interfaces.

```
[SwitchA] display npv login
Server                                                                  External
Interface VSAN FCID     Port WWN                Node WWN                Interface
Vfc1      1    0x010001 21:00:00:00:c8:00:e4:30 20:00:00:00:c8:60:e4:9a Vfc3
Vfc2      1    0x010002 21:00:00:00:c9:00:e4:30 20:00:00:00:c9:60:e4:9a Vfc3
```

The output shows that:

- The domain ID of Switch B is 1.
- Switch B has assigned FC addresses 0x010001 and 0x010002 to Server A and Server B, respectively.

Display the status of Switch A.

```
[SwitchA] display npv status
External Interfaces:
  Interface: Vfc3    VSAN tagging mode: Tagging
    VSAN  State  FCID
    1     Up     0x010000

  Number of External Interfaces: 1

Server Interfaces:
  Interface : Vfc1    VSAN tagging mode: Tagging
    VSAN  State
```

```
  1     Up

Interface : Vfc2    VSAN tagging mode: Tagging
  VSAN  State
  1     Up
```

The output shows that:

- Switch B has assigned FC ID 0x010000 to VFC 3 of Switch A.
- Switch A has one uplink interface (VFC 3) and two downlink interfaces (VFC 1 and VFC 2).

Configuration files

- Switch A:

```
#
 fcoe-mode npv
#
 lldp global enable
#
 system-working-mode advance
#
vsan 1
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
```

```
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr af1 group 1 byte-count 1
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc1
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
interface Vfc2
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/2
#
interface Vfc3
 fc mode np
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/3
#
```

```
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
```

- Switch B:

```
#
 fcoe-mode fcf
#
 system-working-mode advance
#
vsan 1
 zone default-zone permit
#
vlan 10
 fcoe enable vsan 1
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 10
 priority-flow-control enable
 priority-flow-control no-drop dot1p 3
 qos trust dot1p
#
interface Vfc3
 port trunk vsan 1
 bind interface Ten-GigabitEthernet1/0/1
#
```

FIPS configuration examples

This chapter provides configuration examples for logging in to a FIPS device through Stelnet after manual reboot is used to enter FIPS mode.

Example: Logging in to a FIPS device through Stelnet

Applicable product matrix

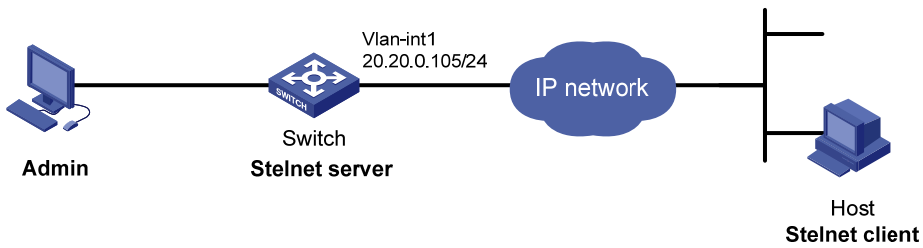
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 75, the administrator is connected to the switch through a console port, and the switch operates in non-FIPS mode.

- Use manual reboot to enter FIPS mode.
- Install the Stelnet client software (use PuTTY0.58 in this example) on the host for logging in to the switch through Stelnet.
- Configure the switch to authenticate the host in password mode.

Figure 75 Network diagram



Configuration restrictions and guidelines

When you configure FIPS, follow these restrictions and guidelines:

- Before the device enters FIPS mode, you must delete the FIPS-incompliant local user service types Telnet and FTP.
- After the **fips mode enable** command is executed, the system prompts you to choose a reboot method. If you do not make a choice within 30 seconds, the system uses the manual reboot method.
- Before you reboot the device to enter FIPS mode, the system automatically removes all key pairs configured in non-FIPS mode and all FIPS-incompliant digital certificates. FIPS-incompliant digital

certificates are MD5-based certificates with the modulus length of key pairs less than 2048 bits. You cannot log in to the device through SSH after the device enters FIPS mode. To log in to the device in FIPS mode through SSH, first log in to the device through a console port, and then create a key pair for the SSH server.

- The password for entering the device in FIPS mode must comply with the password control policies, such as password length, complexity, and aging policy.
- To use the manual reboot method, after you save the configuration file and specify it as the startup configuration file, you must delete the startup configuration file in binary format, and then reboot the device. Otherwise, the commands that are not supported by FIPS mode, if they are in the configuration file, are restored.
- The system enters an intermediate state between when the **fips mode enable** command is executed and when the system is rebooted. If you choose the manual reboot method, do not execute any commands except for the following commands:
  - **reboot**.
  - **save**.
  - Other commands used for configuration preparation to enter FIPS mode.
- After the password control function is enabled globally, you cannot use the **display** command to view the password of a local user for device management.

Configuration procedures

Entering FIPS mode through manual reboot

1. Enable the password control function globally.
2. Add a local user account for device management, including the following items:
   - A username.
   - A password that must comply with the password control policies.
   - A user role of **network-admin**.
3. Enable FIPS mode.
4. Select the manual reboot method.
5. Save the configuration file and specify it as the startup configuration file.
6. Delete the startup configuration file in binary format (an **.mdb** file).
7. Reboot the device.

Configuring the switch

Enable the password control function globally.

```
[Switch] password-control enable
```

Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to 1.

```
[Switch] password-control composition type-number 4 type-length 1
```

Set the minimum length of user passwords to 15 characters.

```
[Switch] password-control length 15
```

Add a local user account named **test** for device management.

```
[Switch] local-user test class manage
New local user added.
```

Configure the password for the local user as **12345zxcvb!@#$%ZXCVB**.

```
[Switch-luser-manage-test] password simple 12345zxcvb!@#$%ZXCVB
Updating user information. Please wait ... ...
```

Specify the user role as **network-admin**.

```
[Switch-luser-manage-test] authorization-attribute user-role network-admin
```

Specify the service type as **SSH** and **terminal**.

```
[Switch-luser-manage-test] service-type ssh terminal
[Switch-luser-manage-test] quit
```

Enable FIPS mode, and choose the manual reboot method to enter FIPS mode.

```
[Switch] fips mode enable
Create a new start-up configuration file named fips-startup.cfg used for FIPS mode. After
setting the login username and password for logging in the device of FIPS mode, the device
will be rebooted automatically. Are you sure? [Y/N]: n
```

Save the current configuration to the root directory of the storage medium, and specify it as the startup configuration file.

```
[Switch] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
[Switch] quit
```

Delete the startup configuration file in binary format.

```
<Switch> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.
```

Reboot the device.

```
<Switch> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

After the device reboots, enter the username **test** and the password **12345zxcvb!@#$%ZXCVB**. The system prompts you to configure a new password. After you configure the new password, the device enters FIPS mode. The new password must have the following details:

- Different from the previous password.
- Include at least 15 characters.
- Contain uppercase and lowercase letters, digits, and special characters, for example, **QQwwee12345^&*()**.

```
Press ENTER to get started.
login: test
Password:
First login or password reset. For security reason, you need to change your pass
word. Please enter your password.
old password:
```

```
new password:
confirm:
Updating user information. Please wait ... ...
<Switch>
```

Display the current FIPS mode state.

```
<Switch> display fips status
FIPS mode is enabled.
```

Create a 2048-bit RSA key pair.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modulus is (2048 ~ 2048).
It will take a few minutes.Press CTRL+C to abort.
Input the modulus length [default = 2048]:
Generating Keys...
.....................................................+++
.....................................................+++
Create the key pair successfully.
```

Enable the SSH server function.

```
[Switch] ssh server enable
```

Set the user authentication mode to **AAA** and remote login protocol to **ssh** for the Stelnet client.

```
[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
```

Set the service type to **Stelnet** and authentication mode to **password** for the user **test**. (This step is optional.)

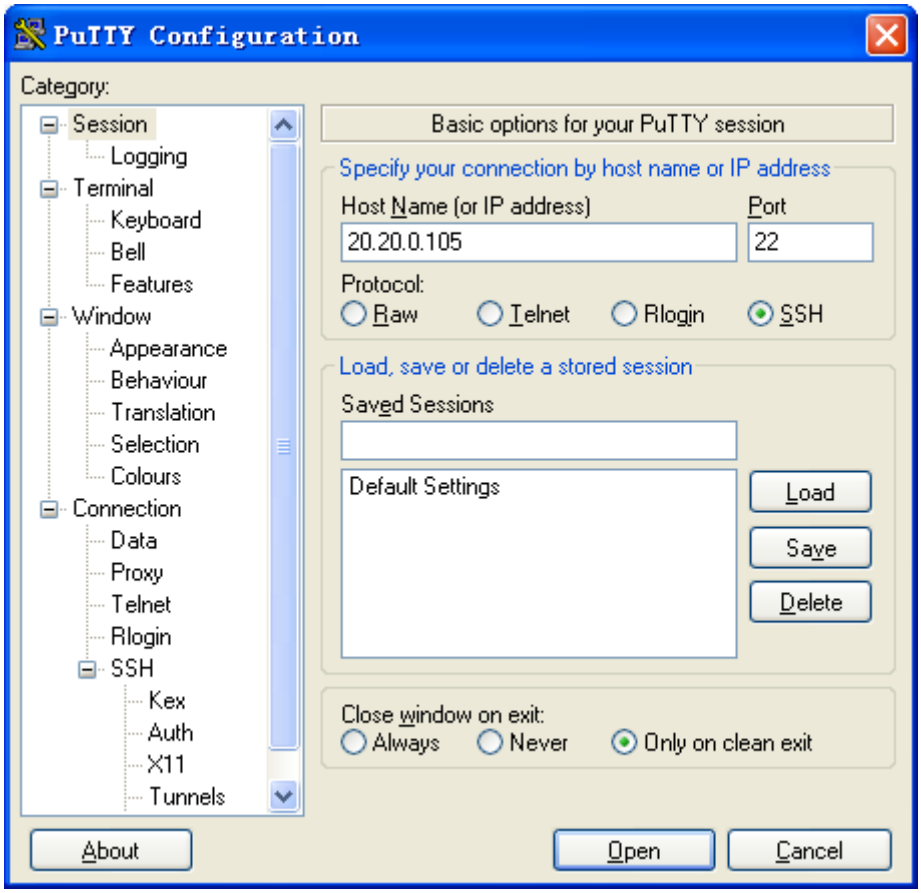
```
[Switch] ssh user test service-type stelnet authentication-type password
```

Configuring the host

1. Install the software PuTTY0.58.
2. Configure an IP address for the Stelnet server.
3. Launch the PuTTY.exe program.

   The **PuTTY Configuration** dialog box appears.

Figure 76 PuTTY configuration



4. In the **Host Name (or IP address)** field, enter the IP address **20.20.0.105**.
5. Click **Open**.

   A security alert dialog box appears to ask you whether you trust this host and want to continue.
6. Click **Yes**.

Verifying the configuration

Verify that the host can use the user name **test** and the password **QQwwee12345^&*()** to log in to the switch after the host establishes a connection to the switch.

```
Login as: test
client001@20.20.0.105's password:
Last successfully login time: Sat Sep  1 08:42:19 2013

******************************************************************************
* 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>
```

Configuration files

```
#
vlan 1
#
interface Vlan-interface1
 ip address 20.20.0.105 255.255.255.0
#
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#
 ssh server enable
 ssh user test service-type stelnet authentication-type password
#
password-control enable
#
local-user test class manage
 service-type ssh terminal
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
 fips mode enable
#
```

IGMP configuration examples

This chapter provides examples for configuring IGMP to manage IP multicast group membership.

Example: Configuring multicast group filters

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

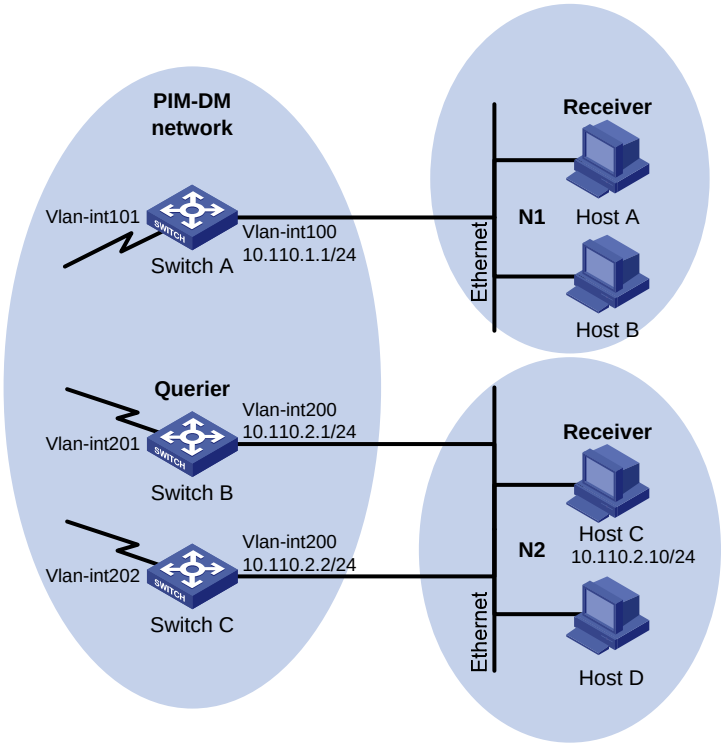
Network requirements

As shown in Figure 77:

- IGMPv2 runs between Switch A and N1, and between the other two switches and N2.
- All switches run OSPF, and they can communicate with each other through unicast routes.

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 77 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Because multiple IGMP-enabled switches exist in N2, you must configure the same multicast group filter on these switches.
- To configure a multicast group filter, you must create a basic ACL, specifying the range of multicast groups that receiver hosts can join.

Configuration restrictions and guidelines

All Layer 3 switches on the same subnet must run the same version of IGMP. Inconsistent versions of IGMP on the Layer 3 switches on the same subnet might lead to inconsistency of IGMP group membership.

Configuration procedures

1. Assign an IP address to each interface in the PIM-DM domain, as shown in Figure 77. (Details not shown.)
2. Enable OSPF on all switches on the PIM-DM network. (Details not shown.)
3. Configure Switch A:

   # Enable IP multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing-enable
   ```

   # Enable IGMP and PIM-DM on 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 on VLAN-interface 101.

   ```
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] pim dm
   [SwitchA-Vlan-interface101] quit
   ```

4. Configure Switch B:

   # Create an ACL rule, specifying the range of multicast groups that receiver hosts can join.

   ```
   <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 configure a multicast group filter that references ACL 2001 on VLAN-interface 200.

   ```
   [SwitchB] interface vlan-interface 200
   [SwitchB-Vlan-interface200] igmp enable
   [SwitchB-Vlan-interface200] igmp group-policy 2001
   ```

   # Enable PIM-DM on VLAN-interface 200.

```
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit
```

Enable PIM-DM on VLAN-interface 201.

```
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

5. Configure Switch C:

Create an ACL rule, specifying the range of multicast groups that receiver hosts can join.

```
<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
```

Enable IGMP, and configure a multicast group filter that references ACL 2001 on VLAN-interface 200.

```
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] igmp group-policy 2001
```

Enable PIM-DM on VLAN-interface 200.

```
[SwitchC-Vlan-interface200] pim dm
[SwitchC-Vlan-interface200] quit
```

Enable PIM-DM on 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
 Vlan-interface200(10.110.2.1):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Querier for IGMP: 10.110.2.1 (This router)
  IGMP groups reported in total: 1
```

Display information about the IGMP querier on Switch C.

```
[SwitchC] display igmp interface
 Vlan-interface200(10.110.2.2):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
```

```
    Other querier present time for IGMP: 255s
    Maximum query response time for IGMP: 10s
    Querier for IGMP: 10.110.2.1
  IGMP groups reported in total: 1
```

The output shows that Switch B with the smaller IP address has become the IGMP querier on this media-shared subnet.

2. Display information about IGMP groups:

   # Send IGMP reports from Host C in N2 to join multicast groups **224.1.1.1** and **224.1.1.2**. (Details not shown.)

   # Display information about IGMP groups on Switch B.

```
[SwitchB] display igmp group
IGMP groups in total: 1
 Vlan-interface200(10.110.2.1):
  IGMP groups reported in total: 1
   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
IGMP groups in total: 1
 Vlan-interface200(10.110.2.2):
  IGMP groups reported in total: 1
   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. The configured multicast group filters have taken effect, and hosts in N2 can join only the multicast group 224.1.1.1.

Configuration files

- Switch A:

```
#
 multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 pim dm
 igmp enable
#
interface Vlan-interface101
 pim dm
#
```

- Switch B:

```
#
 multicast routing-enable
#
acl number 2001
```

```
 rule 0 permit source 224.1.1.1 0
#
vlan 200 to 201
#
interface Vlan-interface200
 pim dm
 igmp enable
 igmp group-policy 2001
#
interface Vlan-interface201
 pim dm
#
```

- Switch C:

```
#
 multicast routing-enable
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200
#
interface Vlan-interface200
 pim dm
 igmp enable
 igmp group-policy 2001
#
interface Vlan-interface202
 pim dm
#
```

IGMP snooping configuration example

This chapter provides examples for configuring IGMP snooping to manage and control multicast group forwarding at Layer 2.

Example: Configuring an IGMP snooping multicast group filter

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

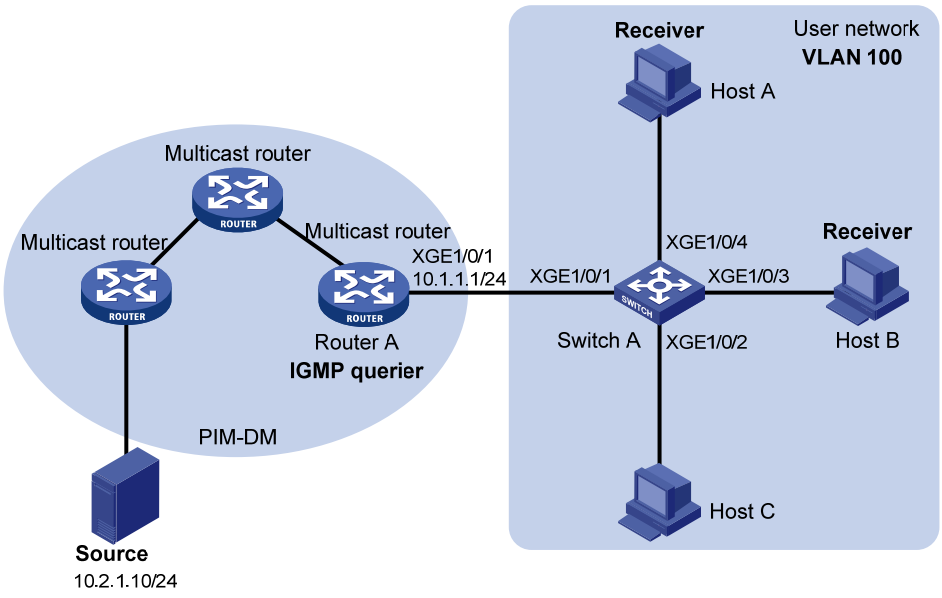
Network requirements

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 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 78 Network diagram



Requirements analysis

To prevent the receiver hosts in VLAN 100 from receiving multicast packets for other multicast groups, you must enable dropping unknown multicast packets for VLAN 100.

To configure a multicast group filter, you must create a basic ACL, specifying the range of the multicast groups that receiver hosts can join.

Configuration restrictions and guidelines

If the ACL for the IGMP snooping multicast group filter does not exist or it 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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port ten-gigabitethernet 1/0/1 to ten-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, specifying the range of the multicast groups that receiver hosts can join.

```
[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 information about IGMP snooping forwarding entries of dynamic multicast groups in VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (1 in total):
      XGE1/0/4         (00:04:10)
```

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 Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Configuring IGMP snooping static ports

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

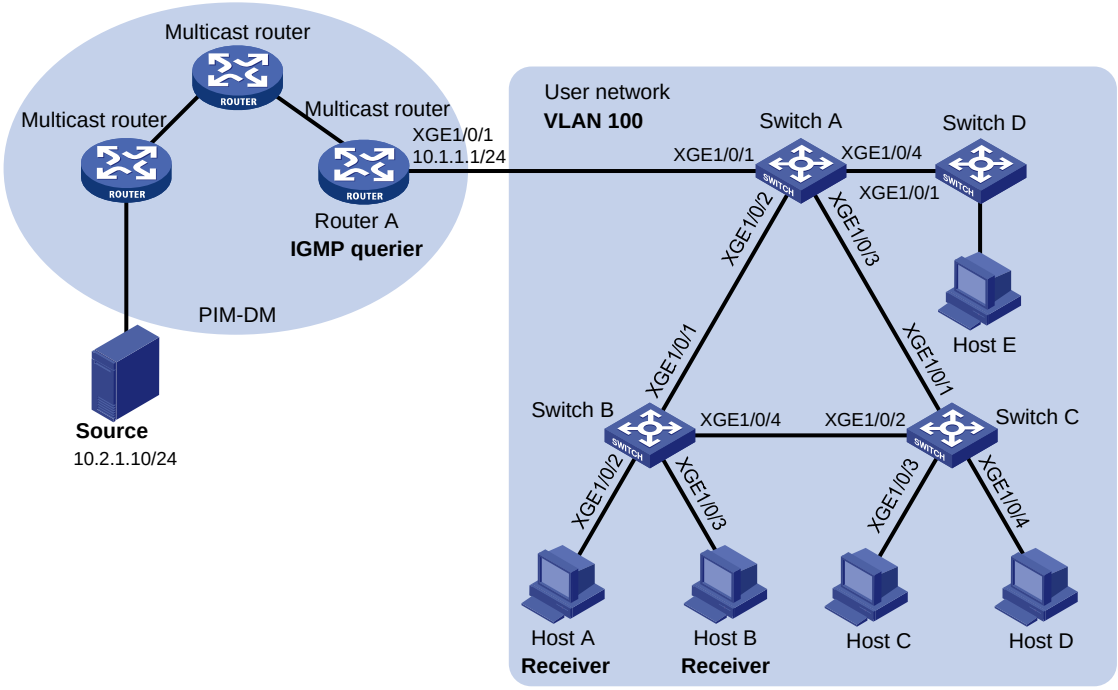
As shown in Figure 79:

- 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 79 Network diagram



Requirements analysis

For the receiver hosts to receive multicast data for a fixed multicast group, you must 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. To implement an immediate switchover to the new path, you must configure all ports that might become multicast data outbound ports as IGMP snooping static router ports.

Configuration procedures

Configuring Switch A

Enable IGMP snooping globally.

```
<SwitchA> system-view
```

```
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 as IGMP snooping static router ports.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchA-Ten-GigabitEthernet1/0/2] quit
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-Ten-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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 as static member ports for the multicast group 224.1.1.1.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-Ten-GigabitEthernet1/0/2] quit
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-Ten-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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchC] vlan 100
```

```
[SwitchC-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/2 as an IGMP snooping static router port.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about IGMP snooping static router ports in VLAN 100 on Switch A and Switch C.

```
[SwitchA] display igmp-snooping static-router-port vlan 100
VLAN 1:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/2
    XGE1/0/3
[SwitchC] display igmp-snooping static-router-port vlan 100
VLAN 1:
  Router slots (0 in total):
  Router ports (1 in total):
    XGE1/0/2
```

The output shows that Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 on Switch A and Ten-GigabitEthernet 1/0/2 on Switch C have become IGMP snooping static router ports.

Display information about IGMP snooping forwarding entries of static multicast groups for VLAN 100 on Switch B.

```
[SwitchB] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 1: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (2 in total):
      XGE1/0/2
      XGE1/0/3
```

The output shows that Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 on Switch B have become the static member ports for the entry (0.0.0.0, 224.1.1.1).

Configuration files

- Switch A:

```
#
 igmp-snooping
#
vlan 100
```

```
 igmp-snooping enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch B:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 igmp-snooping static group 224.1.1.1 vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch C:

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
```

```
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

Information center configuration examples

This document provides information center configuration examples.

The information center receives logs generated by source modules and outputs logs to different destinations according to user-defined output rules.

Logs are classified into eight severity levels from 0 through 7 in descending order. The information center outputs logs with a severity level that is higher than or equal to the specified level. For example, if you specify a severity level of 6 (informational), logs that have a severity level from 0 to 6 are output.

Table 4 Log levels

Severity value	Level	Description
0	Emergency	The system is unusable. For example, the system authorization has expired.
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.
3	Error	Error condition. For example, the link state changes or a storage card is unplugged.
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.
6	Informational	Informational message. For example, a command or a ping operation is executed.
7	Debugging	Debug message.

Example: Outputting logs to a log host

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 80, configure the device to output logs that have a severity level of at least **informational** to the log host.

Figure 80 Network diagram

Configuring the device

Enable the information center.

```
<Device> system-view
[Device] info-center enable
```

Configure an output rule to output logs that have a severity level of at least **informational** to the log host.

```
[Device] info-center source default loghost level informational
```

Specify the IP address of the log host.

```
[Device] info-center loghost 1.2.0.1
```

Verifying the configuration

Display information center configuration on the device.

```
[Device] display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    IP address: 1.2.0.1, port number: 514, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512
    Current messages 512, dropped messages 0, overwritten messages 156
Log file: Enabled
Security log file: Disabled
Information timestamp format:
    Log host: Date
    Other output destination: Date
```

Configuration files

```
#
 info-center loghost 1.2.0.1
#
```

Example: Saving logs into the log file

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

Configure a device to save logs that have a severity level of at least **informational** to the log file.

Configuring the device

Enable the information center.

```
<Device> system-view
[Device] info-center enable
```

Enable saving logs to the log file.

```
[Device] info-center logfile enable
```

Configure an output rule to save logs that have a severity level of at least **informational** to the log file.

```
[Device] info-center source default logfile level informational
```

Set the log file saving interval as 3600 seconds.

```
[Device] info-center logfile frequency 3600
```

Verifying the configuration

Display information center configuration on the device.

```
[Device] display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    IP address: 1.2.0.1, port number: 514, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512
    Current messages 512, dropped messages 0, overwritten messages 156
Log file: Enabled
Security log file: Disabled
Information timestamp format:
    Log host: Date
    Other output destination: Date
```

Display the log file configuration.

```
[Device] display logfile summary
```

```
  Log file: Enabled
  Log file size quota: 10 MB
  Log file directory: flash:/logfile
  Writing frequency: 1 hour 0 min 0 sec
```

Configuration files

```
#
 info-center logfile frequency 3600
#
```

Example: Saving security logs into the security log file

Applicable product matrix

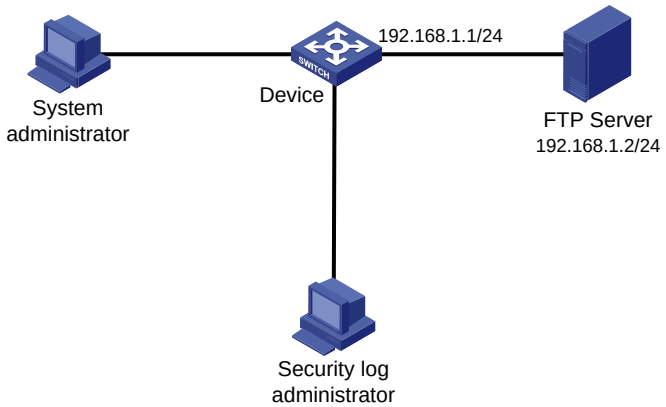
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 81:

- Configure the device to save security logs into the security log file every hour.
- Create a security log administrator user account.
- Log in to the device as the security log administrator to view the security log file contents.
- Back up the security log file to the FTP server.

Figure 81 Network diagram



Configuration restrictions and guidelines

The system administrator and security log administrator have different permissions:

- The system administrator can configure the security log file feature, but cannot manage the security log file.
- The security log administrator can manage the security log file, but cannot configure the security log file feature.

Configuration procedures

Enable the information center.

```
<Device> system-view
[Device] info-center enable
```

Enable saving security logs to the security log file every hour.

```
[Device] info-center security-logfile enable
[Device] info-center security-logfile frequency 3600
```

Create a local user account with username **seclog** and password **seclog123**.

```
[Device] local-user seclog
New local user added.
[Device-luser-manage-seclog] password simple seclog123
```

Authorize the user as the security log administrator.

```
[Device-luser-manage-seclog] authorization-attribute user-role security-audit
```

Authorize the user to use the Telnet service.

```
[Device-luser-manage-seclog] service-type telnet
[Device-luser-manage-seclog] quit
```

Configure the authentication mode of the VTY user interface as **scheme**.

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

Verifying the configuration

Log in to the device by using the user account **seclog**.

```
C:/> telnet 192.168.1.1
******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: seclog
Password:
<Device>
```

Display the contents of the security log file.

```
<Device> more seclog/seclog.log
```

```
%@1%Jan  1 06:49:01:885 2013 Device SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User
=**; Command is local-user seclog
%@2%Jan  1 06:49:08:984 2013 Device SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User
=**; Command is password simple ******
%@3%Jan  1 06:49:15:125 2013 Device SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User
=**; Command is authorization-attribute user-role security-audit
%@4%Jan  1 06:49:29:023 2013 Device SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User
=**; Command is service-type telnet
%@5%Jan  1 06:49:53:266 2013 Device SHELL/5/SHELL_LOGIN: seclog logged in from
192.168.0.5.
```

Back up the security log file onto FTP server 192.168.1.2.

```
<Device> ftp 192.168.0.2
Connected to 192.168.0.2 (192.168.0.2).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.0.2:(none)): admin
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp> put seclog/seclog.log
227 Entering Passive Mode (192,168,0,2,9,54)
150 "D:\seclog\seclog.log" file ready to receive in ASCII mode
226 Transfer finished successfully.
600 bytes sent in 0.000493 seconds (1.16 Mbyte/s)
```

Display the security log configuration.

```
<Device> display security-logfile summary
  Security log file: Enabled
  Security log file size quota: 10 MB
  Security log file directory: flash:/seclog
  Alarm threshold: 80%
  Current usage: 1%
  Writing frequency: 1 hour 0 min 0 sec
```

The output shows that the device saves security logs to the security log file every hour.

Configuration files

- Configurations performed by the system administrator.

```
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
 info-center security-logfile enable
 info-center security-logfile frequency 3600
#
local-user seclog class manage
 password hash $h$6$z8UZoA2AiM1Uwon5$gZ/PGTMrUOgWZ6hsttIQ/3hFHRE3OlGBhyvJlhsFLGM
```

```
ELdFmm/rY2d51I79MAlk+8vVeNyA39ndeB73NBOPefw==
 service-type telnet
 authorization-attribute user-role security-audit
#
```

- Configurations performed by the security log administrator.

  In this example, the commands executed by the security log administrator are not saved to the configuration file.

IP addressing configuration examples

This chapter provides IP addressing configuration examples.

Example: Configuring IP addressing

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

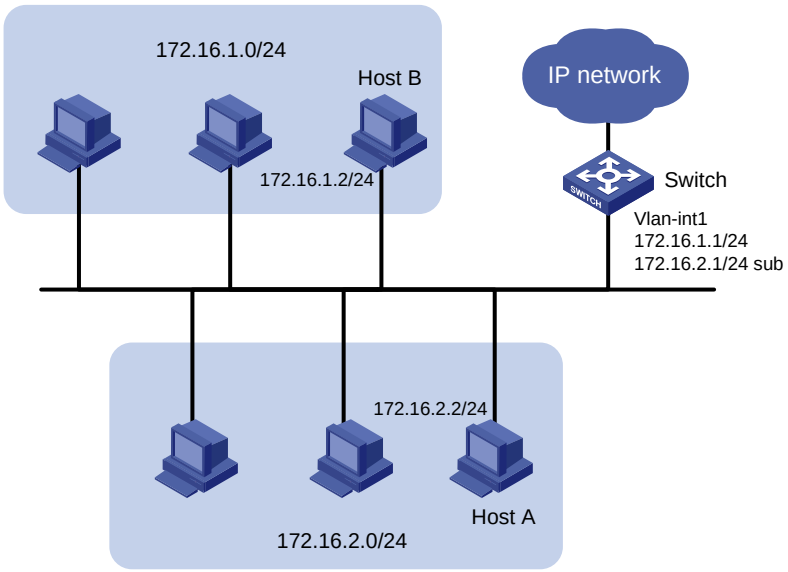
Network requirements

As shown in Figure 82:

- 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 82 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 following gateway addresses on the PCs:
   - Set 172.16.1.1 as the gateway on the PCs attached to subnet 172.16.1.0/24.
   - Set 172.16.2.1 as the gateway 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 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=128 time=7.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=128 time=2.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=128 time=2.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 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 (172.16.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.2.2: icmp_seq=0 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=1 ttl=128 time=7.000 ms
56 bytes from 172.16.2.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.2.2: icmp_seq=3 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 172.16.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 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

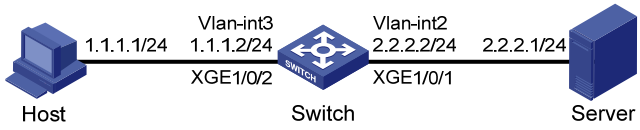
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 83, 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 83 Network diagram



Configuration procedures

1. Configure the switch:

   # Create VLAN 2 and assign Ten-GigabitEthernet 1/0/1 to VLAN 2.

   ```
   <Switch> system-view
   [Switch] Vlan 2
   [Switch-vlan2] port ten-gigabitethernet 1/0/1
   [Switch-Vlan2] quit
   ```

   # Create VLAN 3 and assign Ten-GigabitEthernet 1/0/2 to VLAN 3.

   ```
   [Switch] Vlan 3
   [Switch-vlan3] port ten-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. Verify that the server can receive the ping packets.

Execute the **undo ip forward-broadcast** command on VLAN-interface 2. Verify that the server cannot 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 Ten-GigabitEthernet1/0/1
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 3
#
```

Example: Enabling sending ICMP destination unreachable packets

Applicable product matrix

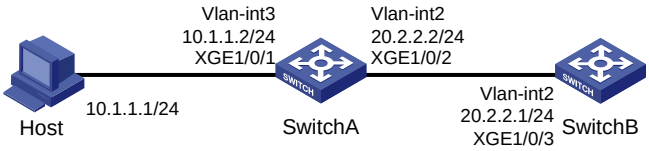
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 84:

- 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 84 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 Ten-GigabitEthernet 1/0/1 to VLAN 3.

   ```
   [SwitchA] Vlan 3
   [SwitchA-vlan3] port ten-gigabitethernet 1/0/1
   [SwitchA-Vlan3] quit
   ```

   # Create VLAN 2 and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

   ```
   [SwitchA] Vlan 2
   [SwitchA-vlan2] port ten-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 Ten-GigabitEthernet 1/0/3 to VLAN 2.

   ```
   <SwitchB> system-view
   [SwitchB] Vlan 2
   [SwitchB-vlan2] port ten-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.

```
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
```

The output shows that:

- The address cannot be pinged from the host.
- Destination unreachable packets are sent back.

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

- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 20.2.2.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 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.

General configuration restrictions and guidelines

IP source guard cannot be configured on a port that is in an aggregate group or service loopback group.

Example: Configuring static IP source guard binding entries

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

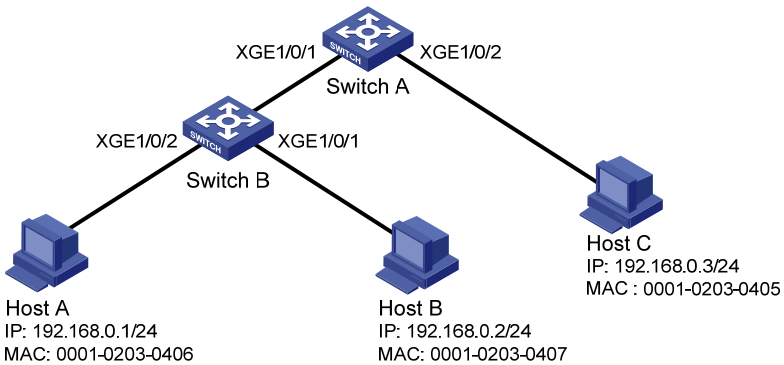
Network requirements

As shown in Figure 85, Host A, B, C, and D use static IP addresses.

Configure static IPv4 source guard binding entries on Switch A and Switch B to meet the following requirements:

- Ten-GigabitEthernet 1/0/1 on Switch A allows only IP packets from Host A to pass.
- Ten-GigabitEthernet 1/0/2 on Switch A and interfaces on Switch B allow only IP packets from their own directly connected hosts to pass.

Figure 85 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable IPv4 source guard on Ten-GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

   ```
   <SwitchA> system-view
   [SwitchA] interface ten-gigabitethernet 1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] ip verify source ip-address mac-address
   ```

   # Bind IP address 192.168.0.3 with MAC address 0001-0203-0405 to form a static IP source guard binding entry on Ten-GigabitEthernet 1/0/2.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3
   mac-address 0001-0203-0405
   [SwitchA-Ten-GigabitEthernet1/0/2] quit
   ```

   # Enable IPv4 source guard on Ten-GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   ```

   # Bind IP address 192.168.0.1 with MAC address 0001-0203-0406 to form a static IP source guard binding entry on Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1
   mac-address 0001-0203-0406
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

2. Configure Switch B:

   # Enable IPv4 source guard on Ten-GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

   ```
   <SwitchB> system-view
   [SwitchB] interface ten-gigabitethernet 1/0/2
   [SwitchB-Ten-GigabitEthernet1/0/2] ip verify source ip-address mac-address
   ```

   # Bind IP address 192.168.0.1 with MAC address 0001-0203-0406 to form a static IP source guard entry on Ten-GigabitEthernet 1/0/2.

   ```
   [SwitchB-Ten-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1
   mac-address 0001-0203-0406
   [SwitchB-Ten-GigabitEthernet1/0/2] quit
   ```

   # Enable IPv4 source guard on Ten-GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

   ```
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   ```

   # Bind IP address 192.168.0.2 with MAC address 0001-0203-0407 to form a static IP source guard binding entry on Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchB-Ten-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2
   mac-address 0001-0203-0407
   [SwitchB-Ten-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
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 XGE1/0/1                N/A  Static
192.168.0.3     0001-0203-0405 XGE1/0/2                N/A  Static
```

Display IPv4 source guard binding entries on Switch B.

```
[SwitchB] display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 XGE1/0/2                N/A  Static
192.168.0.2     0001-0203-0407 XGE1/0/1                N/A  Static
```

Configuration files

- Switch A:

```
#
interface Ten-GigabitEthernet1/0/1
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
#
interface Ten-GigabitEthernet1/0/2
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
#
```

- Switch B:

```
#
interface Ten-GigabitEthernet1/0/1
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0407
#
interface Ten-GigabitEthernet1/0/2
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
#
```

Example: Configuring static and dynamic IP source guard binding entries

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

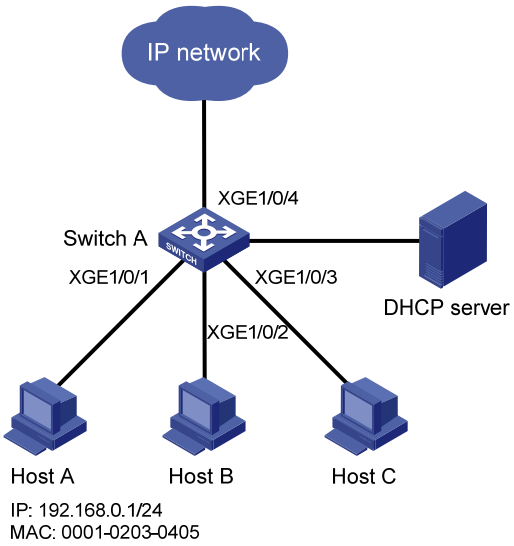
Network requirements

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 IPv4 source guard static and dynamic binding entries on Switch A to meet the following requirements:

- Ten-GigabitEthernet 1/0/1 on Switch A allows only packets from Host A to pass.
- Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 on Switch A allow only packets from Host B and Host C to pass.

Figure 86 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To allow packets from Host A to access the network, bind the IP address and MAC address of Host A. This forms a static IP source guard binding entry on Ten-GigabitEthernet 1/0/1 of Switch A.
- To allow packets from Host B and Host C to access the network, enable IPv4 source guard on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3. IPv4 source guard checks the source IP addresses and MAC addresses of incoming packets based on DHCP snooping entries.

Configuration restrictions and guidelines

To implement dynamic IPv4 source guard, make sure the DHCP snooping function works correctly on the network.

Configuration procedures

Enable IPv4 source guard on Ten-GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
<SwitchA> system-view
```

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Bind IP address 192.168.0.1 with MAC address 0001-0203-0405 to form a static IPv4 source guard binding entry on Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0405
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable DHCP snooping.

```
[SwitchA] dhcp snooping enable
```

Specify GigabitEthernet 1/0/4 as a trusted port.

```
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] dhcp snooping trust
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

Enable IPv4 source guard on Ten-GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/2.

```
[SwitchA-Ten-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Enable IPv4 source guard on Ten-GigabitEthernet 1/0/3 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] ip verify source ip-address mac-address
```

Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/3.

```
[SwitchA-Ten-GigabitEthernet1/0/3] dhcp snooping binding record
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Display IPv4 source guard binding entries.

```
<SwitchA> display ip source binding
Total entries found: 3
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0405 XGE1/0/1                N/A  Static
192.168.0.2     0001-0203-0406 XGE1/0/2                1    DHCP snooping
192.168.0.3     0001-0203-0407 XGE1/0/3                1    DHCP snooping
```

Display DHCP snooping entries.

```
<SwitchA> display dhcp snooping binding
 2 DHCP snooping entries found
 IP Address      MAC Address    Lease        VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 192.168.0.2     0001-0203-0406 16907527     1     N/A    XGE1/0/2
 192.168.0.3     0001-0203-0407 16907528     1     N/A    XGE1/0/3
```

The output shows that dynamic IP source guard obtains DHCP snooping entries.

Configuration files

```
#
 dhcp snooping enable
#
interface Ten-GigabitEthernet1/0/1
ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0405
#
interface Ten-GigabitEthernet1/0/2
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface Ten-GigabitEthernet1/0/3
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface Ten-GigabitEthernet1/0/4
 dhcp snooping trust
#
```

IPsec configuration examples

This chapter provides examples for configuring ACL-based IPsec either manually or by using IKE to protect traffic sourced from and destined for the device.

General configuration restrictions and guidelines

The ACLs for IPsec take effect only on traffic sourced from the device and that destined for the device. They do not take effect on traffic forwarded by the device.

Example: Configuring ACL-based IPsec manually

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 87, establish an ACL-based IPsec tunnel between Switch A and Switch B to protect data flows between the switches, so Switch B can securely transfer the log file to Switch A through FTP.

Configure FTP as follows:

- On Switch A, enable FTP server, create a local FTP user, and configure a user name, a password, and an authorized user role for the FTP user.
- On Switch B, transfer the log file **logfile.log** in the directory **logfile** to Switch A, and save the file as **remotelog.log** in the root directory of Switch A.

Configure the IPsec tunnel as follows:

- Create manual IPsec policies.
- Specify the encapsulation mode as tunnel.
- Specify the security protocol as ESP.
- Specify the encryption algorithm as AES-CBC-192 and authentication algorithm as HMAC-SHA 1.

Figure 87 Network diagram

Requirements analysis

To protect data flows between Switch A and Switch B, perform the following tasks:

- On Switch A, do the following:
  - Configure an ACL to permit packets from Switch A (2.2.2.1) to Switch B (2.2.3.1).
  - Configure a manual IPsec policy.
  - Reference the ACL for the policy.
  - Apply the policy to the VLAN interface.
- On Switch B, do the following:
  - Configure an ACL to permit packets from Switch B (2.2.3.1) to Switch A (2.2.2.1).
  - Configure a manual IPsec policy.
  - Reference the ACL for the policy.
  - Apply the policy to the VLAN interface.

Configuration restrictions and guidelines

Configure an ACL on each switch to define the outbound traffic only. Each ACL rule matches both the outbound traffic and the returned inbound traffic.

Configuration procedures

Before the configuration, make sure Switch A and Switch B can reach each other.

Configuring Switch A

Configure an IP address for interface VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Create a local FTP user, and configure its password as **QQwwee12345^&*()**, authorized user role as **network-admin**, and work directory as root directory.

```
[SwitchA] local-user ftp class manage
New local user added.
[SwitchA-luser-manage-ftp] password simple QQwwee12345^&*()
[SwitchA-luser-manage-ftp] authorization-attribute user-role network-admin
[SwitchA-luser-manage-ftp] authorization-attribute work-directory flash:/
[SwitchA-luser-manage-ftp] service-type ftp
[SwitchA-luser-manage-ftp] quit
```

Enable FTP server.

```
[SwitchA] ftp server enable
[SwitchA] quit
```

Configure an ACL to identify data flows from Switch A to Switch B.

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
```

```
[SwitchA-acl-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[SwitchA] ipsec transform-set tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Specify the security protocol as ESP.

```
[SwitchA-ipsec-transform-set-tran1] protocol esp
```

Specify the ESP encryption algorithm as AES-CBC-192 and authentication algorithm as HMAC-SHA 1.

```
[SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-tran1] quit
```

Create a manual IPsec policy entry with the name **map1** and sequence number 10.

```
[SwitchA] ipsec policy map1 10 manual
```

Reference the ACL.

```
[SwitchA-ipsec-policy-manual-map1-10] security acl 3101
```

Reference the IPsec transform set **tran1**.

```
[SwitchA-ipsec-policy-manual-map1-10] transform-set tran1
```

Specify the remote IP address of the IPsec tunnel as 2.2.3.1.

```
[SwitchA-ipsec-policy-manual-map1-10] remote-address 2.2.3.1
```

Configure inbound and outbound SPIs for ESP.

```
[SwitchA-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[SwitchA-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
```

Configure the inbound and outbound SA keys for ESP.

```
[SwitchA-ipsec-policy-manual-map1-10] sa string-key outbound esp simple abcdefg
[SwitchA-ipsec-policy-manual-map1-10] sa string-key inbound esp simple gfedcba
[SwitchA-ipsec-policy-manual-map1-10] quit
```

Apply the IPsec policy to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec apply policy map1
```

Configuring Switch B

Configure an IP address for interface VLAN-interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Configure an ACL to identify data flows from Switch B to Switch A.

```
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[SwitchB] ipsec transform-set tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Specify the security protocol as ESP.

```
[SwitchB-ipsec-transform-set-tran1] protocol esp
```

Specify the ESP encryption algorithm as AES-CBC-192 and authentication algorithm as HMAC-SHA 1.

```
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-tran1] quit
```

Create a manual IPsec policy entry with the name **use1** and sequence number 10.

```
[SwitchB] ipsec policy use1 10 manual
```

Reference the ACL.

```
[SwitchB-ipsec-policy-manual-use1-10] security acl 3101
```

Reference the IPsec transform set **tran1**.

```
[SwitchB-ipsec-policy-manual-use1-10] transform-set tran1
```

Specify the remote IP address of the IPsec tunnel as 2.2.2.1.

```
[SwitchB-ipsec-policy-manual-use1-10] remote-address 2.2.2.1
```

Configure inbound and outbound SPIs for ESP.

```
[SwitchB-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[SwitchB-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
```

Configure the inbound and outbound SA keys for ESP.

```
[SwitchB-ipsec-policy-manual-use1-10] sa string-key outbound esp simple gfedcba
[SwitchB-ipsec-policy-manual-use1-10] sa string-key inbound esp simple abcdefg
[SwitchB-ipsec-policy-manual-use1-10] quit
```

Apply the IPsec policy to VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec apply policy use1
[SwitchB-Vlan-interface1] quit
[SwitchB] quit
```

Change the working directory to the subdirectory **logfile** of the current directory.

```
<SwitchB> cd logfile
```

Display detailed information about the files in the current subdirectory.

```
<SwitchB> dir
Directory of flash:/logfile
   0 -rw-     8104793 Jan 01 2013 02:50:25   logfile.log

524288 KB total (200384 KB free)
```

The output shows that the log file **logfile.log** exists.

Log in to Switch A by using the user name **ftp** and password **QQwwee12345^&*()**.

```
<SwitchB> ftp 2.2.2.1
Connected to 2.2.2.1 (2.2.2.1).
220 FTP service ready.
User (2.2.2.1:(none)): ftp
331 Password required for ftp.
Password:
```

```
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Set the FTP file transfer mode to ASCII.

```
ftp> ascii
200 TYPE is now ASCII
```

Upload the file **logfile.log**, and save the file as **remotelog.log**.

```
ftp> put logfile.log remotelog.log
227 Entering Passive Mode (2,2,2,1,97,0)
150 Accepted data connection
226 File successfully transferred
8209754 bytes sent in 15.7 seconds (511.3 kbyte/s)
```

Terminate the connection to the FTP server Switch A and return to user view.

```
ftp> bye
221-Goodbye. You uploaded 7813 and downloaded 0 kbytes.
221 Logout.
<SwitchB>
```

Verifying the configuration

Use the **dir** command on Switch A to display detailed information about the files and subdirectories in the root directory. The output shows that the file **remotelog.log** exists, which indicates that Switch B has successfully transferred its log file to Switch A. (Details not shown.)

Use the **display ipsec sa** command on Switch A and Switch B to display the IPsec SAs. This example uses Switch A.

```
[SwitchA] display ipsec sa
------------------------------
Interface: Vlan-interface 1
------------------------------

  ----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: manual
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Path MTU: 1427
    Tunnel:
        local  address: 2.2.2.1
        remote address: 2.2.3.1
    Flow:
        as defined in ACL 3101
    [Inbound ESP SA]
      SPI: 54321 (0x0000d431)
      Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
      No duration limit for this SA
```

```
[Outbound ESP SA]
  SPI: 12345 (0x00003039)
  Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
  No duration limit for this SA
```

Configuration files

- Switch A:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy map1
#
acl number 3101
 rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
#
local-user ftp class manage
 password hash $h$6$amh8I6+/j6x03x7t$lrP/4F6Xrg6zIZXoXPAxthwntD4fNjRMkoQBsL2PBnN
/E0epHve0jNI5Od1v8a/wJqezOpmLN1+hf5KH5SX41w==
 service-type ftp
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec policy map1 10 manual
 transform-set tran1
 security acl 3101
 remote-address 2.2.3.1
 sa spi inbound esp 54321
 sa string-key inbound esp cipher $c$3$rXNId7KfWdMTuvtKJz4d/L1cfU3EHjyyg/M=
 sa spi outbound esp 12345
 sa string-key outbound esp cipher $c$3$itXmPlqD73B03dhD6AMAUkrM5iWwjIMoWwo=
#
```

- Switch B:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 2.2.3.1 255.255.255.0
 ipsec apply policy use1
#
acl number 3101
```

```
 rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec policy map1 10 manual
 transform-set tran1
 security acl 3101
 remote-address 2.2.2.1
 sa spi inbound esp 12345
 sa string-key inbound esp cipher $c$3$itXmPlqD73B03dhD6AMAUkrM5iWwjIMoWwo=
 sa spi outbound esp 54321
 sa string-key outbound esp cipher $c$3$rXNId7KfWdMTuvtKJz4d/L1cfU3EHjyyg/M=
#
```

Example: Configuring ACL-based IPsec by using IKE

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 88, establish an ACL-based IPsec tunnel between Switch A and Switch B to protect data flows in between, so Switch B can securely transfer the configuration file to Switch A through FTP.

Configure FTP as follows:

- On Switch A, do the following:
  - Enable FTP server.
  - Create a local FTP user.
  - Configure a user name, a password, and an authorized user role for the FTP user.
- On Switch B, do the following:
  - Transfer the configuration file **basic.cfg** in the root directory to Switch A.
  - Save the file as **remotebasic.cfg** in the root directory of Switch A.

Configure the IPsec tunnel as follows:

- Create IKE-based IPsec policies.
- Create IPsec transform sets with the default settings.
- Use a pre-shared key for authentication.

Figure 88 Network diagram

Requirements analysis

To protect data flows between Switch A and Switch B, you must perform the following tasks:

- On Switch A, do the following:
  - Configure an ACL to permit packets from Switch A (2.2.2.1) to Switch B (2.2.3.1).
  - Configure an IKE-based IPsec policy.
  - Reference the ACL for the policy.
  - Apply the policy to the VLAN interface.
- On Switch B, do the following:
  - Configure an ACL to permit packets from Switch B (2.2.3.1) to Switch A (2.2.2.1).
  - Configure an IKE-based IPsec policy.
  - Reference the ACL for the policy.
  - Apply the policy to the VLAN interface.

Configuration restrictions and guidelines

Configure an ACL on each switch to define the outbound traffic only. Each ACL rule matches both the outbound traffic and the returned inbound traffic.

Configuration procedures

Before the configuration, make sure Switch A and Switch B can reach each other.

Configuring Switch A

Configure an IP address for interface VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Create a local FTP user.

```
[SwitchA] local-user ftp class manage
New local user added.
```

Configure the password as **QQwwee12345^&*()**.

```
[SwitchA-luser-manage-ftp] password simple QQwwee12345^&*()
```

Configure the authorized user role as **network-admin**.

```
[SwitchA-luser-manage-ftp] authorization-attribute user-role network-admin
```

Configure the work directory as root directory.

```
[SwitchA-luser-manage-ftp] authorization-attribute work-directory flash:/
```

Configure the service type as FTP.

```
[SwitchA-luser-manage-ftp] service-type ftp
[SwitchA-luser-manage-ftp] quit
```

Enable FTP server.

```
[SwitchA] ftp server enable
[SwitchA] quit
```

Configure an ACL to identify data flows from Switch A to Switch B.

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchA-acl-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[SwitchA] ipsec transform-set tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Specify the security protocol as ESP.

```
[SwitchA-ipsec-transform-set-tran1] protocol esp
```

Specify the ESP encryption algorithm as AES-CBC-192 and authentication algorithm as HMAC-SHA 1.

```
[SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-tran1] quit
```

Create an IKE keychain named **keychain1**.

```
[SwitchA] ike keychain keychain1
```

Specify the plaintext **12345zxcvb!@#$%ZXCVB** as the pre-shared key to be used with the remote peer at 2.2.3.1.

```
[SwitchA-ike-keychain-keychain1] pre-shared-key address 2.2.3.1 255.255.255.0 key simple
12345zxcvb!@#$%ZXCVB
[SwitchA-ike-keychain-keychain1] quit
```

Create an IKE profile named **profile1**.

```
[SwitchA] ike profile profile1
```

Reference the IKE keychain **keychain1**.

```
[SwitchA-ike-profile-profile1] keychain keychain1
```

Configure the remote peer ID for IKE profile matching as the IP address 2.2.3.1/24.

```
[SwitchA-ike-profile-profile1] match remote identity address 2.2.3.1 255.255.255.0
[SwitchA-ike-profile-profile1] quit
```

Create an IKE-based IPsec policy entry with the name **map1** and sequence number 10.

```
[SwitchA] ipsec policy map1 10 isakmp
```

Specify the remote IP address of the IPsec tunnel as 2.2.3.1.

```
[SwitchA-ipsec-policy-isakmp-map1-10] remote-address 2.2.3.1
```

Reference the ACL.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

Reference the IPsec transform set **tran1**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

Reference the IKE profile **profile1**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[SwitchA-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec apply policy map1
```

Configuring Switch B

Configure an IP address for interface VLAN-interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Configure an ACL to identify data flows from Switch B to Switch A.

```
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] quit
```

Create an IPsec transform set named **tran1**.

```
[SwitchB] ipsec transform-set tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

Specify the security protocol as ESP.

```
[SwitchB-ipsec-transform-set-tran1] protocol esp
```

Specify the ESP encryption algorithm as AES-CBC-192 and authentication algorithm as HMAC-SHA 1.

```
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-tran1] quit
```

Create an IKE keychain named **keychain1**.

```
[SwitchB] ike keychain keychain1
```

Specify the plaintext **12345zxcvb!@#$%ZXCVB** as the pre-shared key to be used with the remote peer at 2.2.2.1.

```
[SwitchB-ike-keychain-keychain1] pre-shared-key address 2.2.2.1 255.255.255.0 key simple
12345zxcvb!@#$%ZXCVB
[SwitchB-ike-keychain-keychain1] quit
```

Create an IKE profile named **profile1**.

```
[SwitchB] ike profile profile1
```

Reference the IKE keychain **keychain1**.

```
[SwitchB-ike-profile-profile1] keychain keychain1
```

Configure the remote peer ID for IKE profile matching as the IP address 2.2.2.1/24.

```
[SwitchB-ike-profile-profile1] match remote identity address 2.2.2.1 255.255.255.0
[SwitchB-ike-profile-profile1] quit
```

Create an IKE-based IPsec policy entry with the name **use1** and sequence number 10.

```
[SwitchB] ipsec policy use1 10 isakmp
```

Specify the remote IP address of the IPsec tunnel as 2.2.2.1.

```
[SwitchB-ipsec-policy-isakmp-use1-10] remote-address 2.2.2.1
```

Reference the ACL.

```
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

Reference the IPsec transform set **tran1**.

```
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set tran1
```

Reference the IKE profile **profile1**.

```
[SwitchB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[SwitchB-ipsec-policy-isakmp-use1-10] quit
```

Apply the IPsec policy to VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec apply policy use1
[SwitchB-Vlan-interface1] quit
[SwitchB] quit
```

Log in to Switch A by using the user name **ftp** and password **QQwwee12345^&*()**.

```
<SwitchB> ftp 2.2.2.1
Connected to 2.2.2.1 (2.2.2.1).
220 FTP service ready.
User (2.2.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Set the FTP file transfer mode to ASCII.

```
ftp> ascii
200 TYPE is now ASCII
```

Upload the file **basic.cfg**, and save the file as **remotebasic.cfg**.

```
ftp> put basic.cfg remotebasic.cfg
227 Entering Passive Mode (2,2,2,1,97,0)
150 Accepted data connection
226 File successfully transferred
4209754 bytes sent in 7.7 seconds (510.3 kbyte/s)
```

Terminate the connection to the FTP server Switch A and return to user view.

```
ftp> bye
221-Goodbye. You uploaded 7813 and downloaded 0 kbytes.
221 Logout.
<SwitchB>
```

Verifying the configuration

Use the **dir** command on Switch A to display detailed information about the files and subdirectories in the root directory. The output shows that the file **remotebasic.cfg** exists, and Switch B has successfully transferred its configuration file to Switch A. (Details not shown.)

Use the **display ike proposal** command on Switch A and Switch B to display the IKE proposals.

```
[SwitchA] display ike proposal
```

```
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
--------------------------------------------------------------------------------

 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400

[SwitchB] display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
--------------------------------------------------------------------------------

 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400
```

Because no IKE proposal is configured, the command displays only the default IKE proposal.

Use the **display ike sa** command on Switch A to display the IKE SAs.

```
[SwitchA] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               2.2.3.1               RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

Use the **display ipsec sa** command on Switch A to display the IPsec SAs.

```
[SwitchA] display ipsec sa
-------------------------------
Interface: Vlan-interface1
-------------------------------

  ----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1427
    Tunnel:
        local  address: 2.2.2.1
        remote address: 2.2.3.1
    Flow:
    sour addr: 2.2.2.1/255.255.255.255  port: 0  protocol: 0
    dest addr: 2.2.3.1/255.255.255.255  port: 0  protocol: 0

    [Inbound ESP SAs]
      SPI: 3491473451 (0xd01ba82b)
      Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3484
```

```
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for nat traversal: N
      Status: active

    [Outbound ESP SAs]
      SPI: 399193207 (0x17cb3477)
      Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/3484
      Max sent sequence-number: 11
      UDP encapsulation used for nat traversal: N
      Status: active
```

Use the **display ike sa** command on Switch B to display the IKE SAs.

```
[SwitchB] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               2.2.2.1               RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

Use the **display ipsec sa** command on Switch B to display the IPsec SAs.

```
[SwitchB] display ipsec sa
-------------------------------
Interface: Vlan-interface1
-------------------------------

  ----------------------------
  IPsec policy: use1
  Sequence number: 10
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1427
    Tunnel:
        local  address: 2.2.3.1
        remote address: 2.2.2.1
    Flow:
    sour addr: 2.2.3.1/255.255.255.255  port: 0  protocol: 0
    dest addr: 2.2.2.1/255.255.255.255  port: 0  protocol: 0

    [Inbound ESP SAs]
      SPI: 399193207 (0x17cb3477)
      Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/3135
```

```
  Max received sequence-number: 11
  Anti-replay check enable: Y
  Anti-replay window size: 64
  UDP encapsulation used for nat traversal: N
  Status: active

[Outbound ESP SAs]
  SPI: 3491473451 (0xd01ba82b)
  Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3135
  Max sent sequence-number: 4
  UDP encapsulation used for nat traversal: N
  Status: active
```

Configuration files

- Switch A:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy map1
#
acl number 3101
 rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
#
local-user ftp class manage
 password hash $h$6$amh8I6+/j6x03x7t$lrP/4F6Xrg6zIZXoXPAxthwntD4fNjRMkoQBsL2PBnN
/E0epHve0jNI5Od1v8a/wJqezOpmLN1+hf5KH5SX41w==
 service-type ftp
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3101
 remote-address 2.2.3.1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
```

```
 match remote identity address 2.2.3.1 255.255.255.0
#
ike keychain keychain1
 pre-shared-key address 2.2.3.1 255.255.255.0 key cipher $c$3$p6g9j9AdHRhon
Mmm2DPiD+h072CimdWt/DFy5AFFDMXjd3LNuh6n
#
```

- Switch B:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 2.2.3.1 255.255.255.0
 ipsec apply policy use1
#
acl number 3101
 rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3101
 remote-address 2.2.2.1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 match remote identity address 2.2.2.1 255.255.255.0
#
ike keychain keychain1
 pre-shared-key address 2.2.2.1 255.255.255.0 key cipher $c$3$swMEtAyl3cCez
0qj3V2ML1NWrx3fMy0YxI0FfXXTNXPbcGxtQJHK
#
```

IPv6 basics configuration examples

This chapter provides configuration examples for basic IPv6 settings.

Example: Configuring basic IPv6 settings

Applicable product matrix

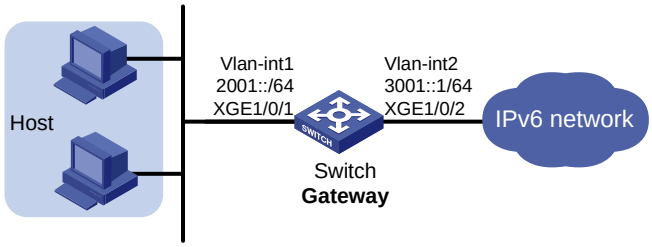
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 89, 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. They also generate the default routes to the switch.

Figure 89 Network diagram



Configuration procedures

1. Configure the switch:

   # Specify an EUI-64 IPv6 address for VLAN-interface 1.

   ```
   [Switch] interface vlan-interface 1
   [Switch-Vlan-interface1] ipv6 address 2001::/64 eui-64
   ```

   # Disable RA message suppression on VLAN-interface 1. By default, no interface advertises RA messages.

   ```
   [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 ten-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. Use the **cmd** command on each host to enter the DOS environment, and then enable IPv6 for the host.

```
C:\Documents and Settings\aa>ipv6 install
```

NOTE:

Because IPv6 is preinstalled, you can skip the host configuration for computers that are running Windows 7 or later versions.

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 [TENTATIVE]
  Global unicast address(es):
    2001::223:89FF:FE5F:958C, subnet is 2001::/64 [TENTATIVE] [EUI-64]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF5F:958c
  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 [TENTATIVE]
  Global unicast address(es):
    3001::1, subnet is 3001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF5F:958C
  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

```
#
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 Ten-GigabitEthernet1/0/2
 port access vlan 2
#
```

IPv6 multicast forwarding over a GRE tunnel configuration examples

This chapter provides examples for configuring IPv6 multicast forwarding over a GRE tunnel.

Example: Configuring IPv6 multicast forwarding over a GRE tunnel

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

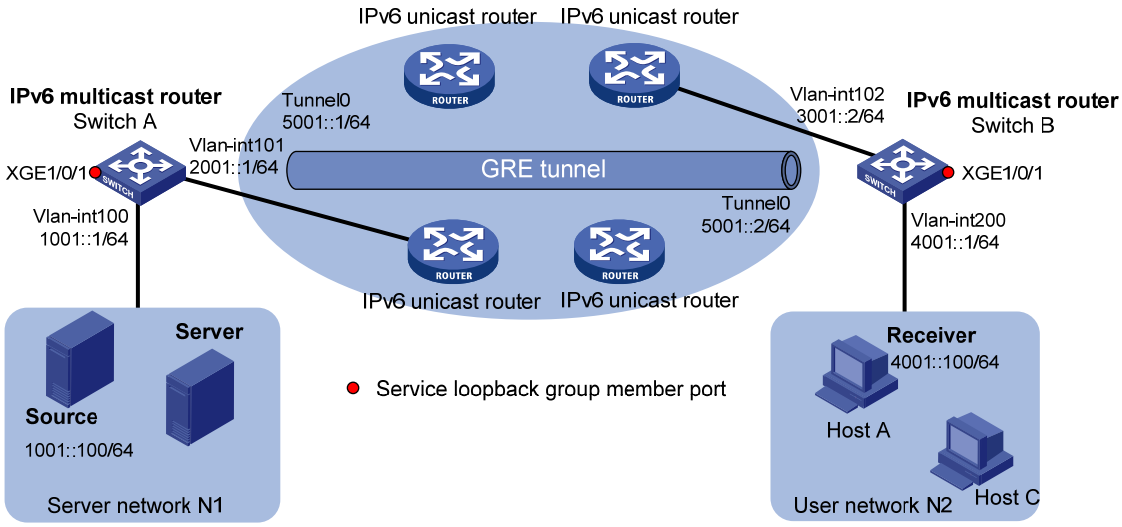
Network requirements

As shown in Figure 90:

- 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 IPv6 multicast. Switch A and Switch B support IPv6 multicast and run IPv6 PIM-DM.
- All routers and switches are interoperable through IPv6 unicast routes.

Configure a GRE over IPv6 tunnel between Switch A and Switch B, so Host A in N2 can receive IPv6 multicast packets from the source in N1.

Figure 90 Network diagram



Configuration restrictions and guidelines

When you configure IPv6 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 IPv6 unicast route.
- The source address and destination address of a tunnel uniquely identify a channel. You must specify the source address and destination address for a tunnel at one end, and reverse the setting at the other end.
- You can configure a static unicast route for forwarding the IPv6 multicast data through the GRE tunnel on the devices at both ends of the tunnel. The destination address of the static route at one end is the IPv6 address of the interface that is connected to the private network at the other end. The next hop address is the IPv6 address of the tunnel interface at the other end. You can also configure a dynamic routing protocol on the tunnel interfaces and the interfaces that are directly connected to the private network to create a dynamic unicast route.
- During the configuration, create a service loopback group, specify its service type as **Tunnel**, and add unused Layer 2 Ethernet ports to the service loopback group.

Configuration procedures

1. Configure the IPv6 address and prefix length for each interface as shown in Figure 90. (Details not shown.)
2. Enable OSPFv3 on routers to make sure both of the following conditions occur: (Details not shown.)
   - The network layer among the routers is interoperable.
   - The routing information among the routers can be dynamically updated.
3. Configure a GRE over IPv6 tunnel:

   # On Switch A, create interface Tunnel 0 and specify the tunnel encapsulation mode as GRE over IPv6.

```
<SwitchA> system-view
[SwitchA] interface tunnel 0 mode gre ipv6
```

Assign an IPv6 address and prefix length to interface Tunnel 0, and specify its source and destination addresses.

```
[SwitchA-Tunnel0] ipv6 address 5001::1 64
[SwitchA-Tunnel0] source 2001::1
[SwitchA-Tunnel0] destination 3001::2
[SwitchA-Tunnel0] quit
```

Create service loopback group 1 and specify its service type as **Tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Add Ten-GigabitEthernet 1/0/1 to service loopback group 1. Ten-GigabitEthernet 1/0/1 is an unused interface and does not belong to VLAN 100 or VLAN 101.

```
[SwitchA] service-loopback group 1 type tunnel
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

On Switch B, create interface Tunnel 0 and specify the tunnel encapsulation mode as GRE over IPv6.

```
<SwitchB> system-view
[SwitchB] interface tunnel 0 mode gre ipv6
```

Assign an IPv6 address and prefix length to interface Tunnel 0 and specify its source and destination addresses.

```
[SwitchB-Tunnel0] ipv6 address 5001::2 64
[SwitchB-Tunnel0] source 3001::2
[SwitchB-Tunnel0] destination 2001::1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1 and specify its service type as **Tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Add Ten-GigabitEthernet 1/0/1 to service loopback group 1. Ten-GigabitEthernet 1/0/1 is an unused interface and does not belong to VLAN 102 or VLAN 200.

```
[SwitchB] service-loopback group 1 type tunnel
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

4. Configure OSPFv3:

Configure OSPFv3 on Switch A and configure its router ID as 1.1.1.1.

```
<SwitchA> system-view
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 0
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ospfv3 1 area 0
[SwitchA-Vlan-interface101] quit
[SwitchA] interface tunnel 0 mode gre ipv6
```

```
[SwitchA-Tunnel0] ospfv3 1 area 0
[SwitchA-Tunnel0] quit
```

Configure OSPFv3 on Switch B and configure its router ID as 2.2.2.2.

```
<SwitchB> system-view
[SwitchB] ospfv3
[SwitchB-ospf-1] router-id 2.2.2.2
[SwitchB-ospf-1] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] ospfv3 1 area 0
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 0
[SwitchB-Vlan-interface200] quit
[SwitchB] interface tunnel 0 mode gre ipv6
[SwitchB-Tunnel0] ospfv3 1 area 0
[SwitchB-Tunnel0] quit
```

5. Enable IPv6 multicast routing, PIM-DM, and MLD:

On Switch A, enable IPv6 multicast routing globally.

```
[SwitchA] ipv6 multicast routing-enable
```

Enable IPv6 PIM-DM on the interfaces through which the IPv6 multicast data passes.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 pim dm
[SwitchA-Tunnel0] quit
```

On Switch B, enable IPv6 multicast routing globally.

```
[SwitchB] ipv6 multicast routing-enable
```

Enable MLD on VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
```

Enable IPv6 PIM-DM on the interfaces through which the multicast data passes.

```
[SwitchB-Vlan-interface200] ipv6 pim dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 pim dm
[SwitchB-Tunnel0] quit
```

Verifying the configuration

Send an MLD report from Host A to join the IPv6 multicast group **FF1E::101**. (Details not shown.)

Send IPv6 multicast data from the IPv6 multicast source to the IPv6 multicast group FF1E::101. (Details not shown.)

Display IPv6 PIM routing table information on Switch B.

```
[SwitchB] display ipv6 pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, FF1E::101)
    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: Vlan200
            Protocol: mld, UpTime: 00:04:25, Expires: -

(1001::100, FF1E::101)
    Protocol: pim-dm, Flag: ACT
    UpTime: 00:06:14
    Upstream interface: Tunnel0
        Upstream neighbor: FE80::A01:101:1
        RPF prime neighbor: FE80::A01:101:1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlan200
            Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

The output shows that Switch A is the RPF neighbor of Switch B and the IPv6 multicast data from Switch A is delivered over a GRE tunnel to Switch B.

Configuration files

- Switch A:

```
#
service-loopback group 1 type tunnel
#
ipv6 multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 1001::1/64
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 address 2001::1/64
#
interface Ten-GigabitEthernet1/0/1
 port service-loopback group 1
#
interface Tunnel0 mode gre ipv6
```

```
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 source 2001::1
 destination 3001::2
 ipv6 address 5001::1/64
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
```

- Switch B:

```
#
service-loopback group 1 type tunnel
#
ipv6 multicast routing-enable
#

vlan 102
#
vlan 200
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 address 3001::2/64
#
interface Vlan-interface200
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 4001::1/64
 mld enable
#
interface Ten-GigabitEthernet1/0/1
 port service-loopback group 1
#
interface Tunnel0 mode gre ipv6
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 source 3001::2
 destination 2001::1
 ipv6 address 5001::2/64
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
```

IPv6 PIM configuration examples

This chapter provides IPv6 PIM configuration examples.

General configuration restrictions and guidelines

All the interfaces on a switch must operate in the same IPv6 PIM mode.

Example: Configuring IPv6 PIM-DM

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 91:

- All the switches are Layer 3 switches.
- 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 91 Network diagram

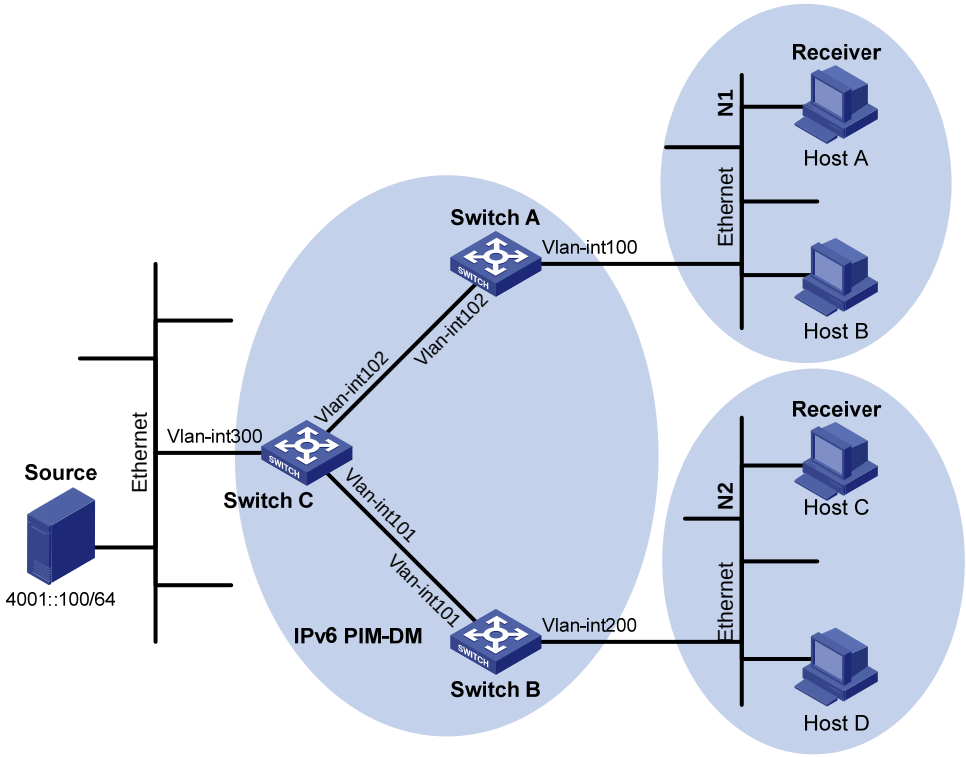


Table 5 Interface and IPv6 address assignment

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. Assign an IPv6 address and prefix length to each interface according to Table 5. (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-DM domain to make sure the following conditions are met: (Details not shown.)

- The switches are interoperable at the network layer.
- The switches can dynamically update their routing information.

3. Enable IPv6 multicast routing and IPv6 PIM-DM:

   # On Switch A, enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6 multicast routing-enable
   ```

   # On Switch A, enable IPv6 PIM-DM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] ipv6 pim dm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 102
   [SwitchA-Vlan-interface102] ipv6 pim 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.)

4. Enable MLD on the interfaces that connect 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

Send MLDv1 reports from Host A and Host C to join the IPv6 multicast group **FF0E::101**. (Details not shown.)

Send IPv6 multicast data from the IPv6 multicast source **4001::100/64** to the IPv6 multicast group **FF0E::101**. (Details not shown.)

Display information about the IPv6 PIM routing table on Switch C.

```
[SwitchC] display ipv6 pim 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: Vlan101
             Protocol: pim-dm, UpTime: 00:02:19, Expires: -
         2: Vlan102
             Protocol: pim-dm, UpTime: 00:02:19, Expires: -
```

Display information about the IPv6 PIM routing table on Switch A.

```
[SwitchA] display ipv6 pim 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: Vlan100
             Protocol: mld, UpTime: 00:01:20, Expires: -

 (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: Vlan100
             Protocol: pim-dm, UpTime: 00:01:20, Expires: -
```

Display information about the IPv6 PIM routing table on Switch B.

```
[SwitchB] display ipv6 pim 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: Vlan200
             Protocol: mld, UpTime: 00:01:20, Expires: -

 (4001::100, FF0E::101)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:01:20
     Upstream interface: Vlan-interface101
         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: Vlan200
        Protocol: pim-dm, UpTime: 00:01:20, Expires: -
```

The output shows the following:

- 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 routing-enable
#
vlan 100
#
vlan 102
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 1001::1/64
 mld enable
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 1002::1/64
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
```

- Switch B:

```
#
 ipv6 multicast routing-enable
#
vlan 101
#
vlan 200
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 2002::1/64
#
interface Vlan-interface200
```

```
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 2001::1/64
 mld enable
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
```

- Switch C:

```
#
 ipv6 multicast routing-enable
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 2002::2/64
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 1002::2/64
#
interface Vlan-interface300
 ospfv3 1 area 0.0.0.0
 ipv6 pim dm
 ipv6 address 4001::1/64
#
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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 92:

- All the switches are Layer 3 switches.
- The IPv6 multicast source, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.

Configure IPv6 PIM-SM on each switch, so that IPv6 multicast data of the IPv6 multicast groups in the range of **FF0E::/64** can be sent to receivers in **N1** and **N2**.

Figure 92 Network diagram

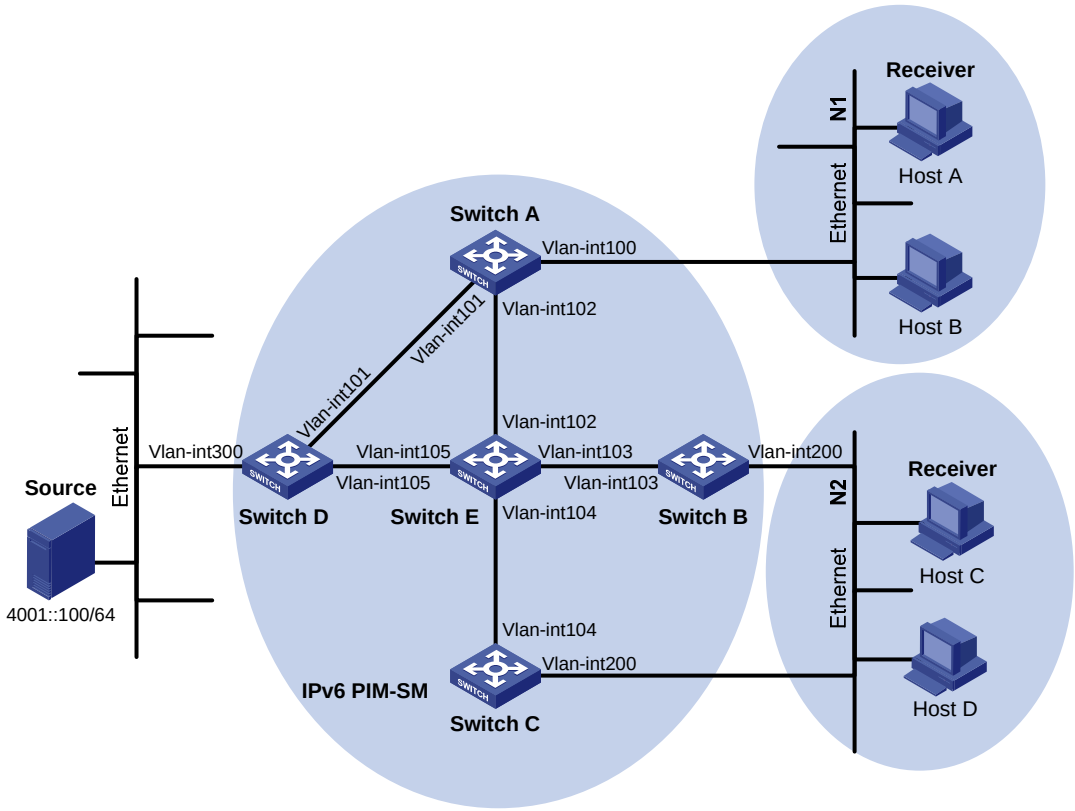


Table 6 Interface and IPv6 address assignment

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

Device	Interface	IPv6 address
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

To meet the network requirements, you must perform the following tasks:

- Because receivers request IPv6 multicast data of the IPv6 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:

- On a shared-media network with multiple Layer 3 switches connected, you can configure MLD and IPv6 PIM-SM on each Layer 3 switch to avoid communication interruption. 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 IPv6 address and prefix length to each interface according to Table 6. (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain to make sure the following conditions are met: (Details not shown.)
   - The switches are interoperable at the network layer.
   - The switches can dynamically update their routing information.
3. Enable IPv6 multicast routing globally and configure IPv6 PIM-SM:

   # On Switch A, enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6 multicast routing-enable
   ```

   # On Switch A, enable IPv6 PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ipv6 pim sm
[SwitchA-Vlan-interface102] quit
```

On Switches B, C, D, and E, enable IPv6 multicast routing and IPv6 PIM-SM in the same way Switch A is configured. (Details not shown.)

4. Enable MLD on the interfaces that connect 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.)

5. 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-BSR, and set its hash mask length to 128 and priority to 10.

```
[SwitchD] ipv6 pim
[SwitchD-pim6] c-bsr 4002::1 hash-length 128 priority 10
```

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-pim6] c-rp 4002::1 group-policy 2005
[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-BSR, and set its hash mask length to 128 and priority to 20.

```
[SwitchE] ipv6 pim
[SwitchE-pim6] c-bsr 1003::2 hash-length 128 priority 20
```

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-pim6] c-rp 1003::2 group-policy 2005
```

```
[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
Vlan-interface200(FE80::223:89FF:FE5F:958B):
   MLD is enabled
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Querier for MLD: FE80::223:89FF:FE5F:958B (this router)
   MLD groups reported in total: 1
```

   # Display MLD querier information on Switch C.

```
[SwitchC] display mld interface
 Vlan-interface200(FE80::223:89FF:FE5F:958C):
   MLD is enabled
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Querier for MLD: FE80::223:89FF:FE5F:958B
   MLD groups reported in total: 1
```

   The output shows that Switch B is elected as 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 ipv6 pim interface
 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 ipv6 pim interface
 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 as 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**. (Details not shown.)

   b. Send IPv6 multicast data from the IPv6 multicast source **4001::100/64** to the IPv6 multicast group **FF0E::100**. (Details not shown.)

c. Display IPv6 PIM routing table information on the switches. Switches A ,D, and E are used as examples.

Display information about the IPv6 PIM routing table on Switch A.

```
[SwitchA] display ipv6 pim routing-table
 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: Vlan100
             Protocol: mld, UpTime: 00:02:15, Expires: -

 (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: Vlan100
             Protocol: pim-sm, UpTime: 00:02:15, Expires: -
```

Display information about the IPv6 PIM routing table on Switch D.

```
[SwitchD] display ipv6 pim routing-table
 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: Vlan101
             Protocol: mld, UpTime: 00:14:44, Expires: -
```

Display information about the IPv6 PIM routing table on Switch E.

```
[SwitchE] display ipv6 pim routing-table
 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: Vlan102
             Protocol: pim-sm, UpTime: 00:16:56, Expires: -

 (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 IPv6 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 initiates a switchover 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 routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1001::1/64
 mld enable
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
```

```
 ipv6 address 1002::1/64
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1003::1/64
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
```

- Switch B:

```
#
ipv6 multicast routing-enable
#
vlan 103
#
vlan 200
#
interface Vlan-interface103
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2002::1/64
#
interface Vlan-interface200
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2001::1/64
 mld enable
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
```

- Switch C:

```
#
ipv6 multicast routing-enable
#
vlan 104
#
vlan 200
#
interface Vlan-interface104
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 3001::1/64
#
interface Vlan-interface200
```

```
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2001::2/64
 mld enable
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
```

- Switch D:

```
#
ipv6 multicast routing-enable
#
acl ipv6 number 2005
 rule 0 permit source FF0E::/64
#
vlan 101
#
vlan 105
#
vlan 300
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1002::2/64
#
interface Vlan-interface105
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 4002::1/64
#
interface Vlan-interface300
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 4001::1/64
#
ipv6 pim
 c-bsr 4002::1 priority 10 hash-length 128
 c-rp 4002::1 group-policy 2005
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
#
```

- Switch E:

```
#
ipv6 multicast routing-enable
```

```
#
acl ipv6 number 2005
 rule 0 permit source FF0E::/64
#
vlan 102 to 104
#
vlan 105
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1003::2/64
#
interface Vlan-interface103
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2002::2/64
#
interface Vlan-interface104
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 3001::2/64
#
interface Vlan-interface105
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 4002::2/64
#
ipv6 pim
 c-bsr 1003::2 priority 20 hash-length 128
 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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 93:

- All switches are Layer 3 switches.
- The IPv6 multicast sources, receiver hosts, and switches can communicate with each other through IPv6 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 IPv6 multicast data only to these IPv6 multicast groups. Receivers in each admin-scoped zone can request IPv6 multicast data only within the local zone.
- Source 3 in the global-scoped zone sends IPv6 multicast data to all IPv6 multicast groups with the scope field value of **14**. All receivers on the network can request IPv6 multicast data of these IPv6 multicast groups.

Figure 93 Network diagram

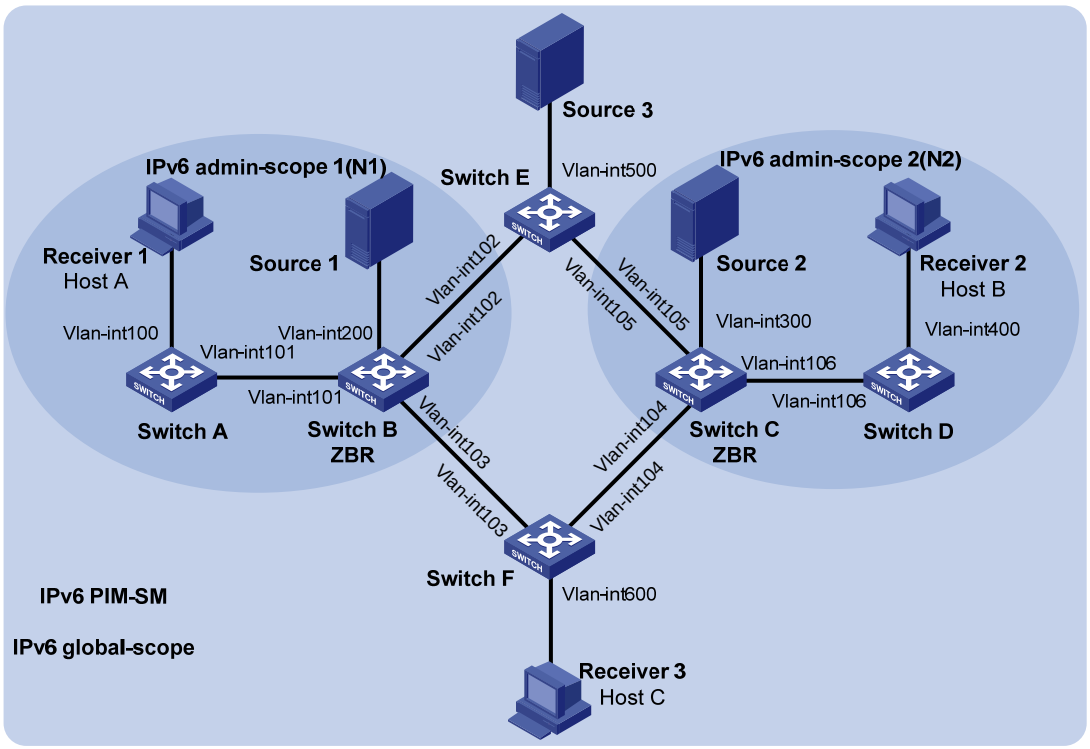


Table 7 Interface and IPv6 address assignment

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

Device	Interface	IPv6 address	Device	Interface	IPv6 address
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	—	2001::100/64
Switch C	VLAN-interface 105	1006::1/64	Source 2	—	3001::100/64
Switch C	VLAN-interface 106	1007::1/64	Source 3	—	5001::100/64
Switch D	VLAN-interface 400	4001::1/64			

Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Configure the boundaries of each admin-scoped zone on the interfaces through which it connects other zones. Make the configuration based on the division of admin-scoped zones and the IPv6 multicast group range to which each zone is designated.
- To make the admin-scoped zones and the global-scoped zone 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

To establish and maintain IPv6 multicast group membership at Layer 3, enable MLD on the interfaces through which the switches are directly connected to receiver hosts.

Configuration procedures

1. Assign an IPv6 address and prefix length to each interface according to Table 7. (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain to make sure the following conditions are met: (Details not shown.)
   - The switches are interoperable at the network layer.
   - The switches can dynamically update their routing information.
3. Enable IPv6 multicast routing and IPv6 PIM-SM:

   # On Switch A, enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6 multicast routing-enable
   ```

   # On Switch A, enable IPv6 PIM-SM on each interface.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] ipv6 pim sm
   ```

```
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 pim sm
[SwitchA-Vlan-interface101] quit
```

On Switches B, C, D, E, and F, enable IPv6 multicast routing, IPv6 administrative scoping, and IPv6 PIM-SM in the same way Switch A is configured. (Details not shown.)

4. Enable MLD on the interfaces that connect 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.)

5. 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] ipv6 multicast boundary scope 4
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] ipv6 multicast boundary scope 4
[SwitchB-Vlan-interface103] quit
```

On Switch C, configure VLAN-interface 104 and VLAN-interface 105 as the boundaries of IPv6 admin-scoped zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] ipv6 multicast boundary scope 4
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 105
[SwitchC-Vlan-interface105] ipv6 multicast boundary scope 4
[SwitchC-Vlan-interface105] quit
```

6. Configure C-BSRs and C-RPs:

On Switch B, configure VLAN-interface 101 as a C-BSR and a C-RP for IPv6 admin-scoped zone 1.

```
[SwitchB] ipv6 pim
[SwitchB-pim6] c-bsr 1002::2 scope 4
[SwitchB-pim6] c-rp 1002::2 scope 4
[SwitchB-pim6] quit
```

On Switch C, configure VLAN-interface 104 as a C-BSR and a C-RP for IPv6 admin-scoped zone 2.

```
[SwitchC] ipv6 pim
[SwitchC-pim6] c-bsr 1007::1 scope 4
[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] ipv6 pim
[SwitchE-pim6] c-bsr 1003::2 scope 14
[SwitchE-pim6] c-rp 1003::2 scope 14
[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:

   # Display BSR information on Switch B.

```
[SwitchB] display ipv6 pim bsr-info
   Scope: non-scoped
     State: Accept Any

   Scope: 4
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 1002::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:04:54
     Candidate BSR address: 1002::2
       Priority: 64
       Hash mask length: 126

   Scope: 14
     State: Accept Preferred
     Bootstrap timer: 00:02:00
     Elected BSR address: 1003::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:02:08
```

   # Display BSR information on Switch C.

```
[SwitchC] display ipv6 pim bsr-info
   Scope: non-scoped
     State: Accept Any

   Scope: 4
     State: Elected
     Bootstrap timer: 00:01:06
     Elected BSR address: 1007::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:04:51
     Candidate BSR address: 1007::1
       Priority: 64
       Hash mask length: 126
```

```
   Scope: 14
     State: Accept Preferred
     Bootstrap timer: 00:02:10
     Elected BSR address: 1003::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:08
```

Display BSR information on Switch E.

```
[SwitchE] display ipv6 pim bsr-info
   Scope: non-scoped
     State: Accept Any

   Scope: 14
     State: Elected
     Bootstrap timer: 00:00:39
     Elected BSR address: 1003::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:31
     Candidate BSR address: 1003::2
       Priority: 64
       Hash mask length: 126
```

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 ipv6 pim rp-info
   BSR RP information:
   Scope: 4
     Group/MaskLen: FF04::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF14::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF24::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
……
   Scope: 14
     Group/MaskLen: FF0E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1001::1                  192       180       00:08:36  00:02:00
     Group/MaskLen: FF1E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1001::1                  192       180       00:08:36  00:02:00
     Group/MaskLen: FF2E::/16
       RP address               Priority  HoldTime  Uptime    Expires
```

```
      1001::1                 192       180       00:08:36  00:02:00
```

……

The output for **FF34::/16** to **FFF4::/16** and **FF3E::/16** to **FFFE::/16** is not shown.

Display RP information on Switch C.

```
[SwitchC] display ipv6 pim rp-info
   BSR RP information:
   Scope: 4
     Group/MaskLen: FF04::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1007::1 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF14::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1007::1 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF24::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1007::1 (local)          192       180       00:02:03  00:02:56
```

……

```
   Scope: 14
     Group/MaskLen: FF0E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1001::1                  192       180       00:08:36  00:02:00
     Group/MaskLen: FF1E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1001::1                  192       180       00:08:36  00:02:00
     Group/MaskLen: FF2E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1001::1                  192       180       00:08:36  00:02:00
```

……

The output for **FF34::/16** to **FFF4::/16** and **FF3E::/16** to **FFFE::/16** is not shown.

Display RP information on Switch E.

```
[SwitchE] display ipv6 pim rp-info
   BSR RP information:
   Scope: 14
     Group/MaskLen: FF0E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1003::2 (local)          192       180       00:07:23  00:02:40
     Group/MaskLen: FF1E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1003::2 (local)          192       180       00:07:23  00:02:40
     Group/MaskLen: FF2E::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1003::2 (local)          192       180       00:07:23  00:02:40
```

……

The output for **FF3E::/16** to **FFFE::/16** is not shown.

Display RP information on Switch F.

```
[SwitchF] display ipv6 pim rp-info
   BSR RP information:
```

```
   Scope: 14
     Group/MaskLen: FF0E::/16
       RP address                Priority  HoldTime  Uptime    Expires
       1003::2                   192       180       00:07:23  00:02:40
     Group/MaskLen: FF1E::/16
       RP address                Priority  HoldTime  Uptime    Expires
       1003::2                   192       180       00:07:23  00:02:40
     Group/MaskLen: FF2E::/16
       RP address                Priority  HoldTime  Uptime    Expires
       1003::2                   192       180       00:07:23  00:02:40
……
```

The output for **FF3E::/16** to **FFFE::/16** is not shown.

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 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1001::1/64
 mld enable
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1002::1/64
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
```

- Switch B:

```
#
ipv6 multicast routing-enable
```

```
#
vlan 101 to 103
#
vlan 200
#
interface Vlan-interface101
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1002::2/64
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 multicast boundary scope 4
 ipv6 pim sm
 ipv6 address 1003::1/64
#
interface Vlan-interface103
 ospfv3 1 area 0.0.0.0
 ipv6 multicast boundary scope 4
 ipv6 pim sm
 ipv6 address 1004::1/64
#
interface Vlan-interface200
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2001::1/64
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
ipv6 pim
 c-bsr 1002::2 scope 4
 c-rp 1002::2 scope 4
#
```

- Switch C:

```
#
ipv6 multicast routing-enable
#
vlan 104 to 106
#
vlan 300
#
interface Vlan-interface104
 ospfv3 1 area 0.0.0.0
 ipv6 multicast boundary scope 4
 ipv6 pim sm
 ipv6 address 1005::1/64
```

```
#
interface Vlan-interface105
 ospfv3 1 area 0.0.0.0
 ipv6 multicast boundary scope 4
 ipv6 pim sm
 ipv6 address 1006::1/64
#
interface Vlan-interface106
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1007::1/64
#
interface Vlan-interface300
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 3001::1/64
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
ipv6 pim
 c-bsr 1007::1 scope 4
 c-rp 1007::1 scope 4
#
```

- Switch D:

```
#
ipv6 multicast routing-enable
#
vlan 106
#
vlan 400
#
interface Vlan-interface106
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1007::2/64
#
interface Vlan-interface400
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 4001::1/64
 mld enable
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
#
```

- Switch E:

```
#
ipv6 multicast routing-enable
#
vlan 102
#
vlan 105
#
vlan 500
#
interface Vlan-interface102
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1003::2/64
#
interface Vlan-interface105
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1006::2/64
#
interface Vlan-interface500
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 5001::1/64
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
#
ipv6 pim
 c-bsr 1003::2 scope 14
 c-rp 1003::2 scope 14
#
```

- Switch F:

```
#
ipv6 multicast routing-enable
#
vlan 103 to 104
#
vlan 600
#
interface Vlan-interface103
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1004::2/64
#
interface Vlan-interface104
 ospfv3 1 area 0.0.0.0
```

```
 ipv6 pim sm
 ipv6 address 1005::2/64
#
interface Vlan-interface600
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 6001::1/64
 mld enable
#
ospfv3 1
 router-id 6.6.6.6
 area 0.0.0.0
#
```

IRF configuration examples

This chapter provides examples for deploying LACP MAD-enabled four-chassis IRF fabrics and BFD MAD-enabled four-chassis IRF fabrics.

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 5920&5900 Switch Series IRF Configuration Guide*.

IRF fabric size

An HP 5900 or 5920 IRF fabric can contain a maximum of four chassis for software versions earlier than **Release 2210**.

Hardware requirements

You can establish an IRF fabric by using HP 5900 switches, HP 5920 switches, or switches from both series. However, you cannot use these two switch series to establish an IRF fabric with any other switch series.

Software requirements

All IRF member devices must run the same system software 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.

The following are physical ports that can be used for IRF connection:

- **HP 5900 switch**—All 10-GE, SFP+, or QSFP+ ports.
- **HP 5920 switch**—All SFP+ ports.

Selecting transceiver modules and cables

When you select transceiver modules and cables, follow these guidelines:

- Select transceiver modules and cables depending on the connection distance.
  - Use 10-GE twisted pairs to connect 10-GE ports in a short distance.
  - Use SFP+/QSFP+ cables to connect SFP+/QSFP+ ports in a short distance.

- Use SFP+/QSFP+ transceiver modules and fibers to connect SFP+/QSFP+ ports in a long distance.

- 10-GE IRF physical ports and QSFP+ transceiver modules are available only for the HP 5900 switches. For more information about transceiver modules, see the switch installation guide.
- The transceiver modules at the two ends of an IRF link must be the same type.

10-GE port restrictions for the HP 5900AF-48XGT-4QSFP+ Switch

When you use the 10-GE ports on the HP 5900AF-48XGT-4QSFP+ Switch as IRF physical ports, follow these guidelines:

- The 10-GE ports are grouped by port number in order, starting from 1. Each group contains four ports. If you use one port in a group for IRF connection, you must also use all the other ports in the group for IRF connection. However, you can bind them to different IRF ports.
- Before you bind a 10-GE port to an IRF port or remove it from the IRF port, you must shut down all the 10-GE ports in the same group.
- Bring up the ports after you complete the operation.

QSFP+ port restrictions for the HP 5900 switch

You can use a QSFP+ port as an IRF physical port, or use the **using tengige** command to split a QSFP+ port into four 10-GE interfaces.

The following restrictions apply to these 10-GE interfaces:

- You must use all or none of the four 10-GE interfaces as IRF physical ports. The four interfaces can be bound to different IRF ports.
- Before you bind a 10-GE interface to an IRF port or remove it from the IRF port, you must shut down all the 10-GE interfaces of the 40-GE port. If any of the interfaces is in up state, the bind or remove action will fail.
- Bring up the interfaces after you complete the operation.

SFP+ port restrictions for the HP 5900AF-48XG-4QSFP+ Switch, HP 5900AF-48XG-4QSFP+ TAA-compliant Switch, HP 5920AF-24XG Switch, and HP 5920AF-24XG TAA-compliant Switch

When you use the SFP+ ports on the HP 5900AF-48XG-4QSFP+ Switch, HP 5900AF-48XG-4QSFP+ TAA-compliant Switch, HP 5920AF-24XG Switch, and HP 5920AF-24XG TAA-compliant Switch as IRF physical ports, follow these guidelines:

- The SFP+ ports are grouped by port number in order, starting from 1. Each group contains four ports. If you use one port in a group for IRF connection, you must also use all the other ports in the group for IRF connection. However, you can bind them to different IRF ports.
- Before you bind an SFP+ port to an IRF port or remove it from the IRF port, you must shut down all the SFP+ ports in the same group.
- Bring up the ports after you complete the operation.

SFP+ port restrictions for the HP 5900AF-48G-4XG-2QSFP+ Switch

When you use the SFP+ ports on the HP 5900AF-48G-4XG-2QSFP+ Switch as IRF physical ports, follow these guidelines:

- If you use one SFP+ port for IRF connection, you must also use all the other SFP+ port for IRF connection. However, you can bind them to different IRF ports.
- Before you bind an SFP+ port to an IRF port or remove it from the IRF port, you must shut down all the SFP+ ports.
- Bring up the ports after you complete the operation.

Topologies

The IRF fabric can use a daisy chain topology or ring topology. To use the ring topology, you must have at least three member devices.

MAD requirements

You must configure LACP MAD, BFD MAD, ARP MAD, or ND MAD on an IRF fabric.

LACP MAD handles collisions in a different way than BFD MAD, ARP MAD, and ND MAD. To avoid conflicts, do not use LACP MAD together with any of those mechanisms in an IRF fabric. However, you can use BFD MAD, ARP MAD, and ND MAD together.

LACP MAD and BFD MAD are most commonly used. Table 8 shows the comparison of the two MAD mechanisms.

Table 8 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 HP intermediate device that supports extended LACP for MAD.	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.	• No special requirements for 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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

Use a four-chassis HP 5900AF-48XG-4QSFP+ Switch IRF fabric (see Figure 95) to replace the ToR switches (see Figure 94) at the access layer of the data center. The access-layer IRF fabric provides Layer 2 forwarding services.

Run LACP MAD to detect IRF split.

Figure 94 Network diagram before IRF deployment

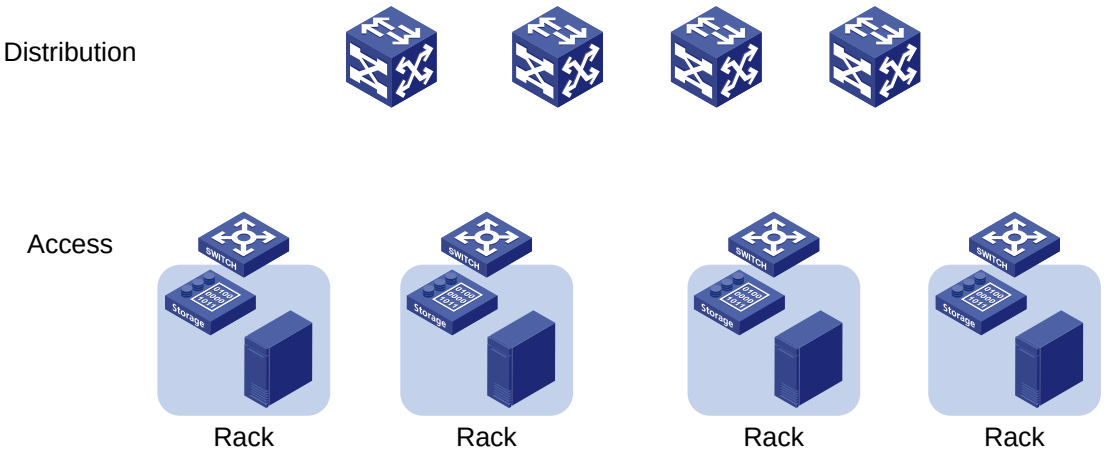
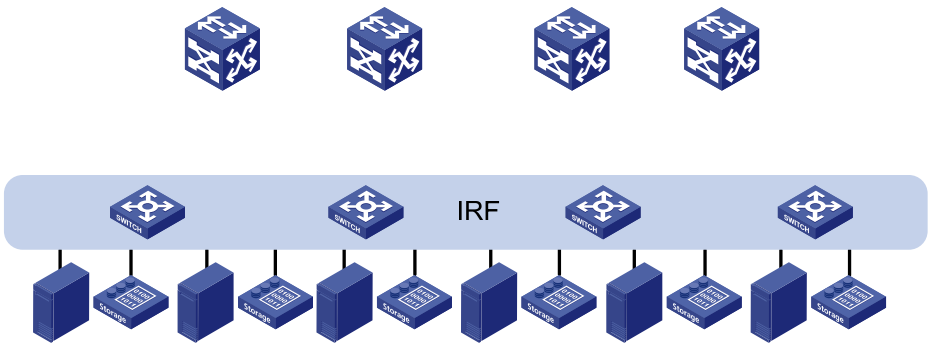


Figure 95 Network diagram after IRF deployment



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, determine the items in Table 9.

Table 9 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 Figure 96).
Member ID assignment	IRF member IDs must be unique.	**Device A**—1. **Device B**—2. **Device C**—3. **Device D**—4.
Master device	IRF members elect a master automatically. For a member device to be elected the master, assign it the highest 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. Use all or none of the physical ports in the same port group for IRF connection. For more information about IRF port bindings, see "General configuration restrictions and guidelines."	See Table 10.

Figure 96 IRF fabric topology

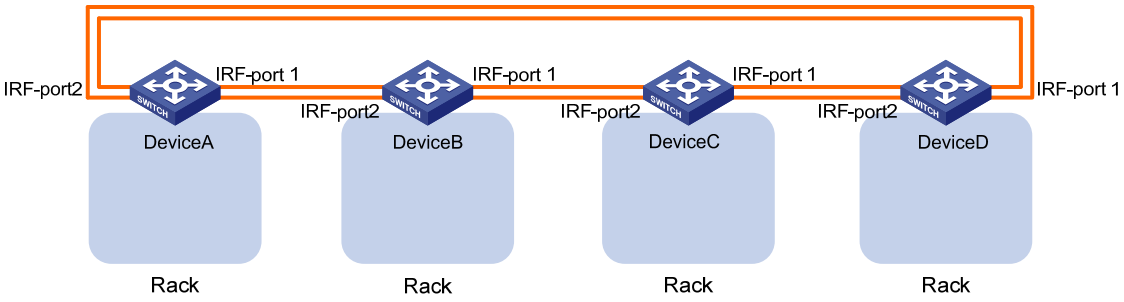


Table 10 IRF physical port bindings

IRF port	IRF physical ports
Device A:	
IRF-port 1	Ten-GigabitEthernet 1/0/25 Ten-GigabitEthernet 1/0/26
IRF-port 2	Ten-GigabitEthernet 1/0/27 Ten-GigabitEthernet 1/0/28

IRF port	IRF physical ports
Device B:	
IRF-port 1	Ten-GigabitEthernet 2/0/25 Ten-GigabitEthernet 2/0/26
IRF-port 2	Ten-GigabitEthernet 2/0/27 Ten-GigabitEthernet 2/0/28
Device C:	
IRF-port 1	Ten-GigabitEthernet 3/0/25 Ten-GigabitEthernet 3/0/26
IRF-port 2	Ten-GigabitEthernet 3/0/27 Ten-GigabitEthernet 3/0/28
Device D:	
IRF-port 1	Ten-GigabitEthernet 4/0/25 Ten-GigabitEthernet 4/0/26
IRF-port 2	Ten-GigabitEthernet 4/0/27 Ten-GigabitEthernet 4/0/28

NOTE:

- The IRF physical ports differ by device models. In this example, 10-GE ports are used for IRF connection.
- The first segment in a physical port number is the IRF member ID. By default, the IRF member ID is 1. Table 10 shows the port numbers after the member IDs are changed.

LACP MAD configuration

IMPORTANT:

For LACP MAD to run correctly, you must make sure the intermediate device supports extended LACPDUs for LACP MAD.

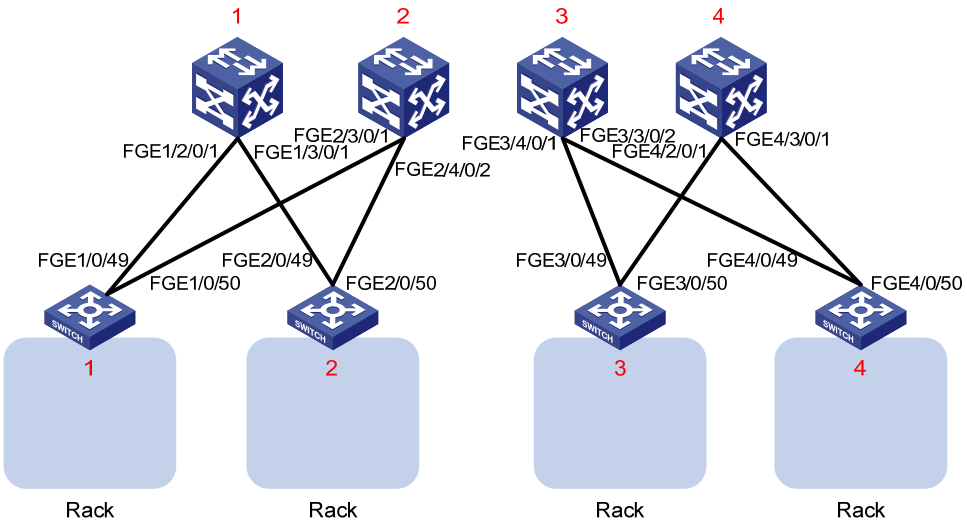
To run LACP MAD, the IRF fabric and intermediate device must each have a dynamic Ethernet link aggregation. LACP MAD cannot run on a static (also called "manual") link aggregation.

If the intermediate device is also an IRF fabric, you must configure MAD for both IRF fabrics, and assign the two IRF fabrics different domain IDs for correct split detection. This example uses a four-chassis IRF fabric at the distribution layer. The access-layer and distribution-layer IRF fabrics are the intermediate device of each other, as shown in Figure 97.

In this example, each member in the access-layer IRF fabric has only two links to the distribution-layer IRF fabric. For high availability, you can connect each member in the access-layer IRF fabric to each member in the distribution-layer IRF fabric. After you aggregate these links, they are regarded as one link in the topology.

For quick split detection, assign high-speed ports for uplink aggregation connections. This example uses 40-GE ports.

Figure 97 LACP MAD



Software feature configuration

In a Layer 2 network, IRF is typically used with link aggregation to simplify the network topology.

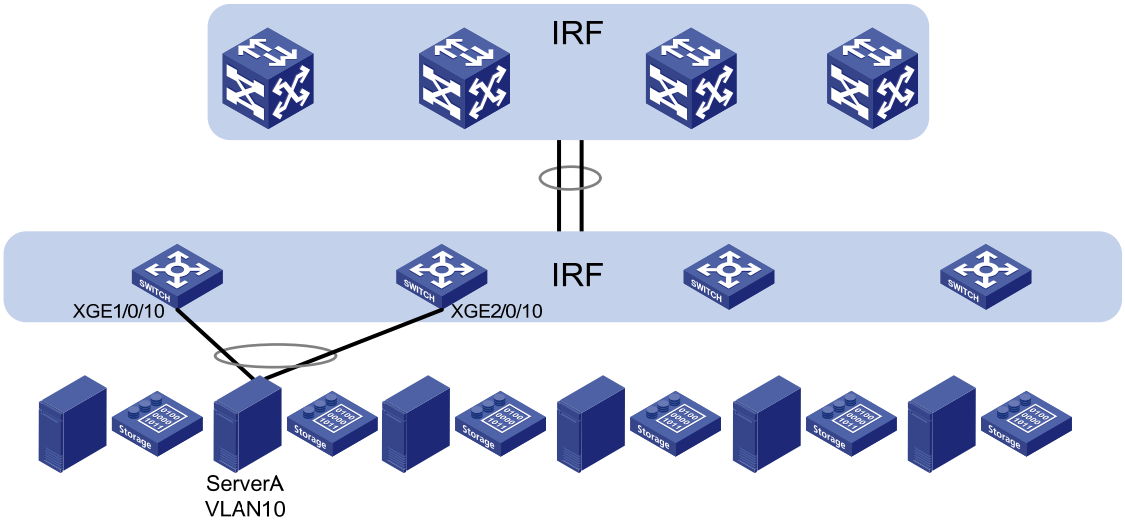
For high availability, you can connect each host or server to two ToR switches in the access-layer IRF fabric, and aggregate the links. On each link aggregation, you do not need to run the spanning tree protocol feature because an IRF fabric appears as one node in the network.

For VLAN tags to be processed correctly, assign ports and aggregate interfaces to the correct VLANs.

NOTE:

A link aggregation could span one member device, some of the member devices, or all member devices, depending on the link redundancy requirements and number of available links. The link aggregation used for LACP MAD must span all member devices.

Figure 98 Connection diagram for the IRF fabrics in a Layer 2 network



Configuration restrictions and guidelines

LACP MAD

When you configure LACP MAD, follow these restrictions and guidelines:

- You only need to run LACP MAD on a single link aggregation for IRF split detection.
- The link aggregation must use dynamic aggregation mode.
- The link aggregation must have at least one member link from each member device.

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 you bind IRF ports.

Configuration procedures

This example assumes that the distribution-layer IRF fabric has been set up.

Setting up the access-layer IRF fabric

1. Configure Device A:

   # Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 1/0/25 to Ten-GigabitEthernet 1/0/28 for IRF connection.

   ```
   <Sysname> system-view
   [Sysname] interface range ten-gigabitethernet 1/0/25 to ten-gigabitethernet 1/0/28
   [Sysname-if-range] shutdown
   [Sysname-if-range] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/25 and Ten-GigabitEthernet 1/0/26 to IRF-port 1/1.

   ```
   [Sysname] irf-port 1/1
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/25
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/26
   [Sysname-irf-port1/1] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/27 and Ten-GigabitEthernet 1/0/28 to IRF-port 1/2.

   ```
   [Sysname] irf-port 1/2
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/27
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/28
   [Sysname-irf-port1/2] quit
   ```

   # Bring up the physical ports.

   ```
   [Sysname] interface range ten-gigabitethernet 1/0/25 to ten-gigabitethernet 1/0/28
   [Sysname-if-range] undo shutdown
   [Sysname-if-range] quit
   ```

   # Assign an IRF member priority of 31 to Device A. This priority is high enough to make sure Device A can be elected as the master.

```
[Sysname] irf member 1 priority 31
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

2. Configure Device B:

Assign member ID 2 to Device B, and reboot the device to effect the member ID change.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 2/0/25 to Ten-GigabitEthernet 2/0/28 for IRF connection.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/25 to ten-gigabitethernet 2/0/28
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 2/0/25 and Ten-GigabitEthernet 2/0/26 to IRF-port 2/1.

```
[Sysname] irf-port 2/1
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/25
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/26
[Sysname-irf-port2/1] quit
```

Bind Ten-GigabitEthernet 2/0/27 and Ten-GigabitEthernet 2/0/28 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/27
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/28
[Sysname-irf-port2/2] quit
```

Bring up the physical ports.

```
[Sysname] interface range ten-gigabitethernet 2/0/25 to ten-gigabitethernet 2/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device B to Device A, as shown in Figure 96.

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

Device B fails master election and reboots. A two-chassis IRF fabric is formed.

3. Configure Device C:

Assign member ID 3 to Device C, and reboot the device to effect the member ID change.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 3/0/25 to Ten-GigabitEthernet 3/0/28 for IRF connection.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 3/0/25 to ten-gigabitethernet 3/0/28
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 3/0/25 and Ten-GigabitEthernet 3/0/26 to IRF-port 3/1.

```
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/25
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/26
[Sysname-irf-port3/1] quit
```

Bind Ten-GigabitEthernet 3/0/27 and Ten-GigabitEthernet 3/0/28 to IRF-port 3/2.

```
[Sysname] irf-port 3/2
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/27
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/28
[Sysname-irf-port3/2] quit
```

Bring up the physical ports.

```
[Sysname] interface range ten-gigabitethernet 3/0/25 to ten-gigabitethernet 3/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device C to Device B, as shown in Figure 96.

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

Device C reboots to join the IRF fabric. A three-chassis IRF fabric is formed.

4. Configure Device D:

Assign member ID 4 to Device D, and reboot the device to effect the member ID change.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 4
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 4/0/25 to Ten-GigabitEthernet 4/0/28 for IRF connection.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 4/0/25 to ten-gigabitethernet 4/0/28
```

```
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 4/0/25 and Ten-GigabitEthernet 4/0/26 to IRF-port 4/1.

```
[Sysname] irf-port 4/1
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/25
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/26
[Sysname-irf-port4/1] quit
```

Bind Ten-GigabitEthernet 4/0/27 and Ten-GigabitEthernet 4/0/28 to IRF-port 4/2.

```
[Sysname] irf-port 4/2
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/27
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/28
[Sysname-irf-port4/2] quit
```

Bring up the ports.

```
[Sysname] interface range ten-gigabitethernet 4/0/25 to ten-gigabitethernet 4/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device D to Device A and Device C, as shown in Figure 96.

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

Configuring LACP MAD

1. Configure the IRF fabric at the access layer:

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] 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
```

Create a named interface range that contains uplink ports to the distribution layer IRF fabric. In this example, the interface range name is **lacp**, and each member has two links to the distribution layer IRF fabric.

```
[Sysname] interface range name lacp interface FortyGigE 1/0/49 to FortyGigE 1/0/50
FortyGigE 2/0/49 to FortyGigE 2/0/50 FortyGigE 3/0/49 to FortyGigE 3/0/50 FortyGigE
4/0/49 to FortyGigE 4/0/50
```

Assign the ports in the interface range to Bridge-Aggregation 2.

```
[Sysname-if-range-lacp] port link-aggregation group 2
```

```
[Sysname-if-range-lacp] quit
```

2. Configure the IRF fabric at the distribution layer:

   # Assign IRF domain ID 2 to the IRF fabric.

```
<Sysname> system-view
[Sysname] irf domain 2
```

   # Create Bridge-Aggregation 2, set its aggregation mode to dynamic, and enable LACP MAD.

```
[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: 2]:
 The assigned  domain ID is: 2
 Info: MAD LACP only enable on dynamic aggregation interface.
[Sysname-Bridge-Aggregation2] quit
```

   # Create a named interface range that contains the downlink ports to the access-layer IRF fabric. The interface range name is **lacp1**, and contains four downlink ports.

```
[Sysname] interface range name lacp1 interface FortyGigE 1/2/0/1 FortyGigE 1/3/0/1
FortyGigE 2/3/0/1 FortyGigE 2/4/0/2
```

   NOTE:

   An interface range can contain a maximum of five port item. Each item can be an individual port or port range. In this example, you must use two interface ranges on the distribution-layer IRF fabric.

   # Assign the ports in the **lacp1** interface range to Bridge-Aggregation 2.

```
[Sysname-if-range-lacp1] port link-aggregation group 2
[Sysname-if-range-lacp1] quit
```

   # Create a named interface range that contains the downlink ports to the access-layer IRF fabric. The interface range name is **lacp2**, and contains the rest of downlink ports.

```
[Sysname] interface range name lacp2 interface FortyGigE 3/4/0/1 FortyGigE 3/3/0/2
FortyGigE 4/2/0/1 FortyGigE 4/3/0/1
```

   # Assign the ports in the **lacp2** interface range to Bridge-Aggregation 2.

```
[Sysname-if-range-lacp2] port link-aggregation group 2
[Sysname-if-range-lacp2] quit
```

Configuring software features

This section provides the VLAN and link aggregation configuration procedure for end devices (for example, a server in VLAN 10).

1. Configure the IRF fabric at the access layer:

   # Create VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
```

   # Create Bridge-Aggregation 3, and set its aggregation mode to dynamic.

```
[Sysname] interface bridge-aggregation 3
[Sysname-Bridge-Aggregation3] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation3] quit
```

Assign Ten-GigabitEthernet 1/0/10 and Ten-GigabitEthernet 2/0/10 to the aggregation group for Bridge-Aggregation 3.

```
[Sysname] interface ten-gigabitethernet 1/0/10
[Sysname-Ten-GigabitEthernet1/0/10] port link-aggregation group 3
[Sysname-Ten-GigabitEthernet1/0/10] quit
[Sysname] interface ten-gigabitethernet 2/0/10
[Sysname-Ten-GigabitEthernet2/0/10] port link-aggregation group 3
[Sysname-Ten-GigabitEthernet2/0/10] quit
```

Assign Bridge-Aggregation 3 to VLAN 10.

```
[Sysname] interface bridge-aggregation 3
[Sysname-Bridge-Aggregation3] port access vlan 10
[Sysname-Bridge-Aggregation3] quit
```

Configure Bridge-Aggregation 2 as a trunk port, and assign it to VLAN 10.

```
[Sysname] interface bridge-aggregation 2
[Sysname-Bridge-Aggregation2] port link-type trunk
[Sysname-Bridge-Aggregation2] port trunk permit vlan 10
[Sysname-Bridge-Aggregation2] quit
```

2. Configure the IRF fabric at the distribution layer:

Create VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
```

Configure Bridge-Aggregation 2 as a trunk port, and assign it to VLAN 10.

```
[Sysname] interface bridge-aggregation 2
[Sysname-Bridge-Aggregation2] port link-type trunk
[Sysname-Bridge-Aggregation2] port trunk permit vlan 10
[Sysname-Bridge-Aggregation2] 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    Role    Priority  CPU-Mac         Description
 *+1        Master  31        0cda-414a-859c  ---
   2        Standby 1         00a0-fc00-5801  ---
   3        Standby 1         0cda-415e-232f  ---
   4        Standby 1         00e0-fc58-1235  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0cda-414a-859b
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 2
```

The output shows that the IRF fabric has four member devices.

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         2             UP         4           0cda-414a-859b
 2           UP         3             UP         1           0cda-414a-859b
 3           UP         4             UP         2           0cda-414a-859b
 4           UP         1             UP         3           0cda-414a-859b
```

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 IP address of the IRF fabric at the distribution layer from a server.

```
C:\Users>ping 10.153.116.111 –t
```

On the IRF fabric at the access layer, shut down Ten-GigabitEthernet 1/0/10, a member port of Bridge-Aggregation 3.

```
[Sysname] interface ten-gigabitethernet 1/0/10
[Sysname-Ten-GigabitEthernet1/0/10] shutdown
[Sysname-Ten-GigabitEthernet1/0/10] quit
```

Observe the output on the server configuration terminal.

```
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.
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 IP address can be pinged after transient traffic disruption.

On the IRF fabric at the access layer, shut down FortyGigE 1/0/49 and FortyGigE 1/0/50 (member ports of Bridge-Aggregation 2). The server cannot access the distribution layer through Device A.

```
[Sysname] interface range FortyGigE 1/0/49 FortyGigE 1/0/50
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Observe the output on the server configuration terminal.

```
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.
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 IP address can be pinged after transient traffic disruption. The server accesses the distribution layer through another device in the access-layer IRF fabric.

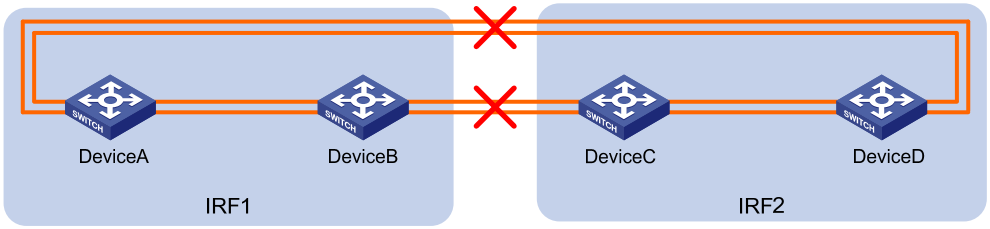
Verifying link failure protection of the ring topology

Disconnect all IRF links between any two IRF member devices to verify that the IRF fabric can operate correctly as a daisy chained fabric. (Details not shown.)

Verifying the LACP MAD configuration

As shown in Figure 99, disconnect two IRF connections: one between Device A and Device D, and the other between Device B and Device C.

Figure 99 IRF split



The disconnect actions cause the IRF fabric to break down into two parts: IRF 1 (Device A and Device B) and IRF 2 (Device C and Device D). The system displays IRF link state and member device failure error messages.

Observe the output messages to verify that LACP MAD take the following actions:

- Changes IRF 2 (Device C and Device D) to the Recovery state, because the master device in IRF 1 has a lower member ID than the master device in IRF 2.
- Shuts down all physical network ports on Device C and Device D, except for the IRF physical ports and ports configured to be excluded from the shutdown action.

The following is the sample output on IRF 1:

```
%Jan  1 05:19:10:176 2011 HP STM/3/STM_LINK_STATUS_DOWN: IRF port 2 is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/27 link status
is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/28 link status
is down.
%Jan  1 05:19:10:176 2011 HP STM/3/STM_LINK_STATUS_DOWN: IRF port 1 is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet2/0/25 link status
is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet2/0/26 link status
is down.
%Jan  1 05:19:10:186 2011 HP DEV/3/BOARD_REMOVED: Board is removed from Slot 3, type is
MAIN_BOARD_TYPE_52QF.
%Jan  1 05:19:10:186 2011 HP DEV/3/BOARD_REMOVED: Board is removed from Slot 4, type is
MAIN_BOARD_TYPE_52QF.
```

The following is the sample output from IRF 2:

```
%Jan  1 05:53:20:784 2011 HP HA/5/HA_STANDBY_TO_MASTER: Standby board in slot 3 changes
to master.
%Jan  1 05:53:20:831 2011 HP DEV/3/BOARD_REMOVED: Board is removed from Slot 1, type is
MAIN_BOARD_TYPE_52QF.
%Jan  1 05:53:20:831 2011 HP DEV/3/BOARD_REMOVED: Board is removed from Slot 2, type is
MAIN_BOARD_TYPE_52QF.
%Jan  1 05:53:20:860 2011 HP DEV/1/MAD_DETECT: Multi-active devices detected, please fix
it.
```

```
%Jan  1 05:53:20:886 2011 HP IFNET/3/PHY_UPDOWN: M-GigabitEthernet0/0/0 link status is
down.
%Jan  1 05:53:20:887 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
M-GigabitEthernet0/0/0 is down.
%Jan  1 05:53:20:912 2011 HP IFNET/3/PHY_UPDOWN: FortyGigE3/0/49 link status is down.
%Jan  1 05:53:20:914 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
FortyGigE3/0/49 is down.
%Jan  1 05:53:20:912 2011 HP IFNET/3/PHY_UPDOWN: FortyGigE3/0/50 link status is down.
%Jan  1 05:53:20:914 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
FortyGigE3/0/49 is down.
%Jan  1 05:53:20:912 2011 HP IFNET/3/PHY_UPDOWN: FortyGigE4/0/49 link status is down.
%Jan  1 05:53:20:914 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
FortyGigE3/0/49 is down.
%Jan  1 05:53:20:912 2011 HP IFNET/3/PHY_UPDOWN: FortyGigE4/0/50 link status is down.
%Jan  1 05:53:20:914 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
FortyGigE3/0/49 is down.
```

The output shows that initially IRF 2 took over the master role because it considered IRF 1 as having failed. LACP MAD shut down the network ports on IRF 2 after it detected an MAD conflict.

If IRF 1 fails, use the **mad restore** command on IRF 2 to recover the member device and bring up all ports that have been shut down by LACP MAD.

NOTE:

You can log in to IRF 2 through the console port on Device C or Device D. If you have excluded a network port from the MAD shutdown action, you can telnet to IRF 2 through the network port.

```
<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]
%Jan  1 05:24:41:249 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet2/0/10 link status
is up.
%Jan  1 05:24:41:249 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet2/0/10 is up.
%Jan  1 05:24:41:325 2011 HP IFNET/3/PHY_UPDOWN: FortyGigE2/0/49 link status is up.
%Jan  1 05:24:41:325 2011 HP IFNET/3/PHY_UPDOWN: FortyGigE2/0/50 link status is up.
%Jan  1 05:24:46:266 2011 HP IFNET/3/PHY_UPDOWN: M-GigabitEthernet0/0/0 link status is
up.
%Jan  1 05:24:46:268 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
M-GigabitEthernet0/0/0 is up.
```

The output shows that network connectivity of IRF 2 has been restored.

Remove all IRF 1 and IRF link failures.

After the link failure of IRF 1 is removed, the IRF ports recover. The following is the sample output on IRF 1:

```
%Jan  1 05:29:06:913 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/27 link status
is up.
%Jan  1 05:29:06:914 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/27 is up.
```

```
%Jan  1 05:29:06:913 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/28 link status
is up.
%Jan  1 05:29:06:914 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/28 is up.
%Jan  1 05:29:07:106 2011 HP STM/6/STM_LINK_STATUS_UP: IRF port 2 is up.
%Jan  1 05:29:07:810 2011 HP STM/4/STM_LINK_RECOVERY: Merge occurs.
```

IRF 2 reboots automatically to merge with IRF 1.

Execute the **display irf** command to verify that the IRF fabric is recovered with Device A as the master.

```
<Sysname> display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  31        0cda-414a-859c  ---
   2        Standby 1         00a0-fc00-5801  ---
   3        Standby 1         0cda-415e-232f  ---
   4        Standby 1         00e0-fc58-1235  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0cda-414a-859b
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 2
```

Configuration files

- IRF fabric at the access layer:

```
#
 irf domain 2
 irf member 1 priority 31
#
vlan 10
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/25
 port group interface Ten-GigabitEthernet1/0/26
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/0/27
 port group interface Ten-GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/0/25
 port group interface Ten-GigabitEthernet2/0/26
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/27
 port group interface Ten-GigabitEthernet2/0/28
#
```

```
irf-port 3/1
 port group interface Ten-GigabitEthernet3/0/25
 port group interface Ten-GigabitEthernet3/0/26
#
irf-port 3/2
 port group interface Ten-GigabitEthernet3/0/27
 port group interface Ten-GigabitEthernet3/0/28
#
irf-port 4/1
 port group interface Ten-GigabitEthernet4/0/25
 port group interface Ten-GigabitEthernet4/0/26
#
irf-port 4/2
 port group interface Ten-GigabitEthernet4/0/27
 port group interface Ten-GigabitEthernet4/0/28
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 10
 link-aggregation mode dynamic
 mad enable
#
interface Bridge-Aggregation3
 port access vlan 10
 link-aggregation mode dynamic
#
interface FortyGigE1/0/49                                                    .
 port link-aggregation group 2
#
interface FortyGigE1/0/50
 port link-aggregation group 2
#
interface FortyGigE2/0/49                                                    .
 port link-aggregation group 2
#
interface FortyGigE2/0/50
 port link-aggregation group 2
#
interface FortyGigE3/0/49                                                    .
 port link-aggregation group 2
#
interface FortyGigE3/0/50
 port link-aggregation group 2
#
interface FortyGigE4/0/49                                                    .
 port link-aggregation group 2
#
interface FortyGigE4/0/50
```

```
 port link-aggregation group 2
#
interface Ten-Gigabitethernet 1/0/10
 port link-aggregation group 3
#
interface Ten-Gigabitethernet 2/0/10
 port link-aggregation group 3
```

- IRF fabric at the distribution layer:

```
#
 irf domain 2
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 10
 link-aggregation mode dynamic
 mad enable
#
interface FortyGigE1/2/0/1
 port link-aggregation group 2
#
interface FortyGigE1/3/0/1
 port link-aggregation group 2
#
interface FortyGigE2/3/0/1
 port link-aggregation group 2
#
interface FortyGigE2/4/0/1
 port link-aggregation group 2
#
interface FortyGigE3/3/0/2
 port link-aggregation group 2
#
interface FortyGigE3/4/0/1
 port link-aggregation group 2
#
interface FortyGigE4/2/0/1
 port link-aggregation group 2
#
interface FortyGigE4/3/0/1
 port link-aggregation group 2
```

Example: Setting up a four-chassis BFD MAD-enabled IRF fabric

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 101, set up a four-chassis HP 5900AF-48XG-4QSFP+ Switch IRF fabric to replace the switches at the distribution layer of the enterprise network (see Figure 100).

Use BFD MAD to detect IRF split because LACP is not available.

The IRF fabric provides gateway services for servers and runs OSPF.

Figure 100 Network diagram before IRF deployment

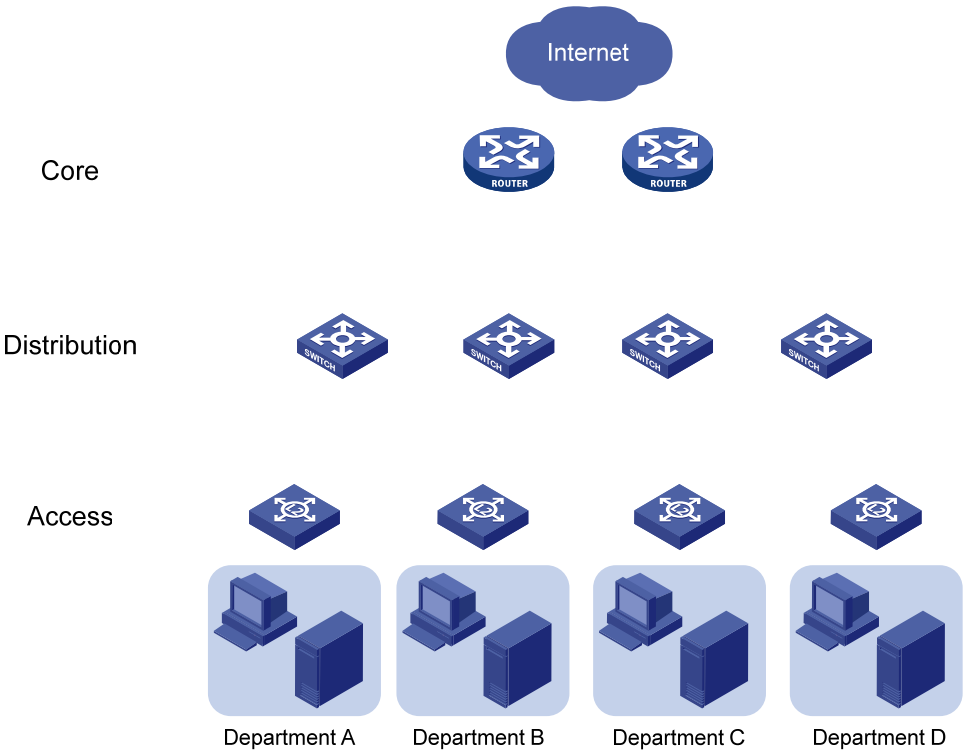
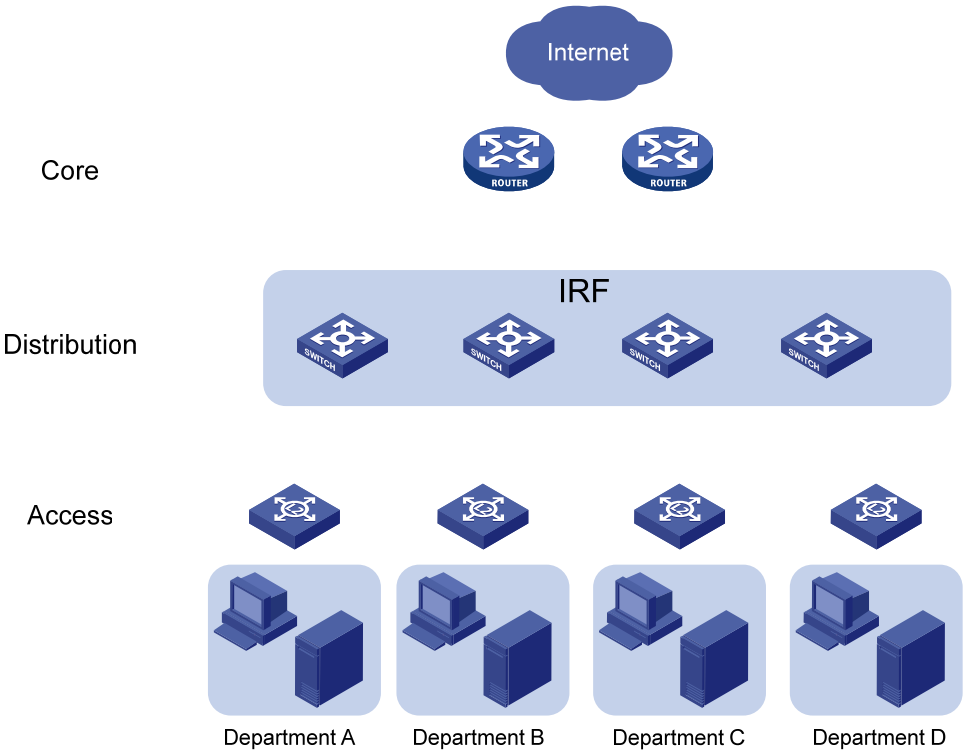


Figure 101 Network diagram after IRF deployment



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, determine the items in Table 11.

Table 11 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 Figure 102).
Member ID assignment	IRF member IDs must be unique.	**Device A**—1. **Device B**—2. **Device C**—3. **Device D**—4.
Master device	IRF members elect a master automatically. For a member device to be elected the master, assign it the highest member priority.	Device A.

Item	Analysis	Choice in this example
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. Use all or none of the physical ports in the same port group for IRF connection. For more information about port binding requirements, see "IRF physical ports and connection requirements."	See Table 12.

Figure 102 IRF fabric topology

Table 12 IRF physical port bindings

IRF port	IRF physical ports
Device A:	
IRF-port 1	Ten-GigabitEthernet 1/0/25 Ten-GigabitEthernet 1/0/26
IRF-port 2	Ten-GigabitEthernet 1/0/27 Ten-GigabitEthernet 1/0/28
Device B:	
IRF-port 1	Ten-GigabitEthernet 2/0/25 Ten-GigabitEthernet 2/0/26
IRF-port 2	Ten-GigabitEthernet 2/0/27 Ten-GigabitEthernet 2/0/28
Device C:	
IRF-port 1	Ten-GigabitEthernet 3/0/25 Ten-GigabitEthernet 3/0/26
IRF-port 2	Ten-GigabitEthernet 3/0/27 Ten-GigabitEthernet 3/0/28
Device D:	

IRF port	IRF physical ports
IRF-port 1	Ten-GigabitEthernet 4/0/25 Ten-GigabitEthernet 4/0/26
IRF-port 2	Ten-GigabitEthernet 4/0/27 Ten-GigabitEthernet 4/0/28

NOTE:

- The IRF physical ports differ by device models. In this example, 10-GE ports are used for IRF connection.
- The first segment in a physical port number is the IRF member ID. By default, the IRF member ID is 1. Table 12 shows the port numbers after the member IDs are changed.

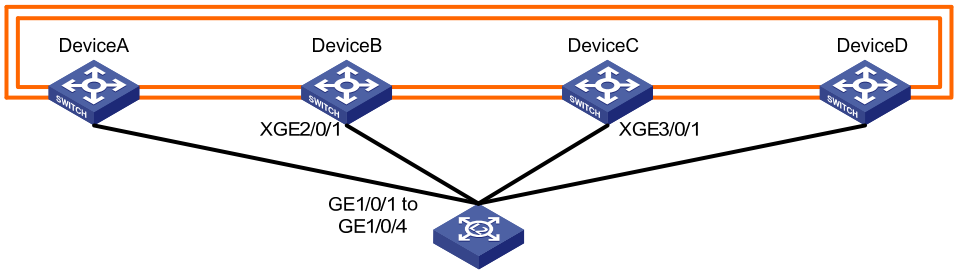
BFD MAD configuration

You can deploy BFD MAD by using one of the following methods:

- Connect all member devices 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 device, as shown in Figure 103. This method is suitable for IRF fabrics that have more than two member devices, because it uses fewer physical ports than the previous method.

The intermediate device forwards BFD MAD packets transparently. You do not need to configure any special settings on the intermediate device except that you must assign all BFD MAD links to the VLAN used for BFD MAD.

Figure 103 BFD MAD connection diagram



Software feature configuration

IRF is typically used with link aggregation to simplify the network topology. For high availability, set up multichassis link aggregations with the downstream switches and the upstream egress routers, as shown in Figure 104. A link aggregation could span one member device, some of the member devices, or all member devices, depending on the link redundancy requirements and number of available links. Because this example does not use LACP MAD, 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 to provide gateway services, as shown in Table 13.

To use the IRF fabric in a Layer 3 network, you must configure routing. In this example, OSPF is configured.

Figure 104 Connection diagram for the IRF fabric in a Layer 3 network

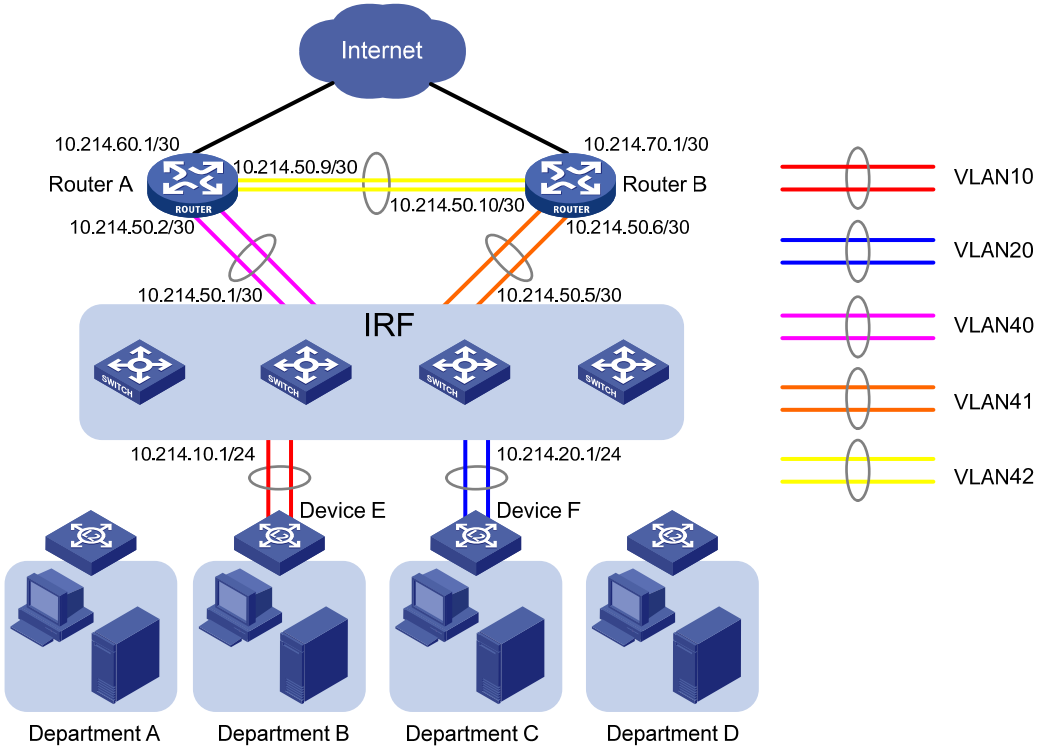


Table 13 Link aggregations and VLAN assignment scheme

Aggregate interface	Member ports	VLANs	VLAN interface's IP address
Router A:			
Bridge-Aggregation 40	Ten-GigabitEthernet 1/0/1 Ten-GigabitEthernet 1/0/2 Ten-GigabitEthernet 1/0/3 Ten-GigabitEthernet 1/0/4	VLAN 40	10.214.50.2/30
Bridge-Aggregation 42	Ten-GigabitEthernet 1/0/5 Ten-GigabitEthernet 1/0/6	VLAN 42	10.214.50.9/30
Router B:			
Bridge-Aggregation 41	Ten-GigabitEthernet 1/0/1 Ten-GigabitEthernet 1/0/2 Ten-GigabitEthernet 1/0/3 Ten-GigabitEthernet 1/0/4	VLAN 41	10.214.50.6/30
Bridge-Aggregation 42	Ten-GigabitEthernet 1/0/5 Ten-GigabitEthernet 1/0/6	VLAN 42	10.214.50.10/30
IRF fabric:			

Aggregate interface	Member ports	VLANs	VLAN interface's IP address
Bridge-Aggregation 10	Ten-GigabitEthernet 1/0/10 Ten-GigabitEthernet 2/0/10 Ten-GigabitEthernet 3/0/10 Ten-GigabitEthernet 4/0/10	VLAN 10	10.214.10.1/24
Bridge-Aggregation 20	Ten-GigabitEthernet 1/0/11 Ten-GigabitEthernet 2/0/11 Ten-GigabitEthernet 3/0/11 Ten-GigabitEthernet 4/0/11	VLAN 20	10.214.20.1/24
Bridge-Aggregation 40	Ten-GigabitEthernet 1/0/13 Ten-GigabitEthernet 2/0/13 Ten-GigabitEthernet 3/0/13 Ten-GigabitEthernet 4/0/13	VLAN 40	10.214.50.1/30
Bridge-Aggregation 41	Ten-GigabitEthernet 1/0/14 Ten-GigabitEthernet 2/0/14 Ten-GigabitEthernet 3/0/14 Ten-GigabitEthernet 4/0/14	VLAN 41	10.214.50.5/30
Device E:			
Bridge-Aggregation 10	Ten-GigabitEthernet 1/0/49 Ten-GigabitEthernet 1/0/50 Ten-GigabitEthernet 1/0/51 Ten-GigabitEthernet 1/0/52	VLAN 10	No VLAN interface is required.
Device F:			
Bridge-Aggregation 20	Ten-GigabitEthernet 1/0/49 Ten-GigabitEthernet 1/0/50 Ten-GigabitEthernet 1/0/51 Ten-GigabitEthernet 1/0/52	VLAN 20	No VLAN interface is required.

Configuration restrictions and guidelines

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. Do not configure an IP address with the **ip address** command or configure a VRRP virtual address on the BFD MAD-enabled VLAN interface. • 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 you bind IRF ports.

Configuration procedures

Setting up the IRF fabric

1. Configure Device A:

   # Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 1/0/25 to Ten-GigabitEthernet 1/0/28 for IRF connection.

   ```
   <Sysname> system-view
   [Sysname] interface range ten-gigabitethernet 1/0/25 to ten-gigabitethernet 1/0/28
   [Sysname-if-range] shutdown
   [Sysname-if-range] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/25 and Ten-GigabitEthernet 1/0/26 to IRF-port 1/1.

   ```
   [Sysname] irf-port 1/1
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/25
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/26
   [Sysname-irf-port1/1] quit
   ```

Bind Ten-GigabitEthernet 1/0/27 and Ten-GigabitEthernet 1/0/28 to IRF-port 1/2.

```
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/27
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/28
[Sysname-irf-port1/2] quit
```

Bring up the physical ports.

```
[Sysname] interface range ten-gigabitethernet 1/0/25 to ten-gigabitethernet 1/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Assign an IRF member priority of 31 to Device A. This priority is high enough to ensure that Device A can be elected as the master.

```
[Sysname] irf member 1 priority 31
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

2. Configure Device B:

Assign member ID 2 to Device B, and reboot the device to effect the member ID change.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 2/0/25 to Ten-GigabitEthernet 2/0/28 for IRF connection.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/25 to ten-gigabitethernet 2/0/28
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 2/0/25 and Ten-GigabitEthernet 2/0/26 to IRF-port 2/1.

```
[Sysname] irf-port 2/1
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/25
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/26
[Sysname-irf-port2/1] quit
```

Bind Ten-GigabitEthernet 2/0/27 and Ten-GigabitEthernet 2/0/28 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/27
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/28
[Sysname-irf-port2/2] quit
```

Bring up the physical ports.

```
[Sysname] interface range ten-gigabitethernet 2/0/25 to ten-gigabitethernet 2/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device B to Device A, as shown in Figure 102.

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

Device B fails master election and reboots. A two-chassis IRF fabric is formed.

3. Configure Device C:

Assign member ID 3 to Device C, and reboot the device to effect the member ID change.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 3/0/25 to Ten-GigabitEthernet 3/0/28 for IRF connection.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 3/0/25 to ten-gigabitethernet 3/0/28
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 3/0/25 and Ten-GigabitEthernet 3/0/26 to IRF-port 3/1.

```
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/25
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/26
[Sysname-irf-port3/1] quit
```

Bind Ten-GigabitEthernet 3/0/27 and Ten-GigabitEthernet 3/0/28 to IRF-port 3/2.

```
[Sysname] irf-port 3/2
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/27
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/28
[Sysname-irf-port3/2] quit
```

Bring up the physical ports.

```
[Sysname] interface range ten-gigabitethernet 3/0/25 to ten-gigabitethernet 3/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device C to Device B, as shown in Figure 102.

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active.
```

Device C reboots to join the IRF fabric. A three-chassis IRF fabric is formed.

4. Configure Device D:

Assign member ID 4 to Device D, and reboot the device to effect the member ID change.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 4
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Shut down the physical ports used for IRF connection. This example uses the port group that contains Ten-GigabitEthernet 4/0/25 to Ten-GigabitEthernet 4/0/28 for IRF connection.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 4/0/25 to ten-gigabitethernet 4/0/28
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 4/0/25 and Ten-GigabitEthernet 4/0/26 to IRF-port 4/1.

```
[Sysname] irf-port 4/1
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/25
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/26
[Sysname-irf-port4/1] quit
```

Bind Ten-GigabitEthernet 4/0/27 and Ten-GigabitEthernet 4/0/28 to IRF-port 4/2.

```
[Sysname] irf-port 4/2
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/27
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/28
[Sysname-irf-port4/2] quit
```

Bring up the physical ports.

```
[Sysname] interface range ten-gigabitethernet 4/0/25 to ten-gigabitethernet 4/0/28
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

Save the running configuration.

```
[Sysname] quit
<Sysname> save
```

Connect Device D to Device C and Device A, as shown in Figure 102.

Activate the IRF port configuration.

```
<Sysname> system-view
[Sysname] irf-port-configuration active
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

Configuring BFD MAD

1. Configure the IRF fabric:

   # Create VLAN 1000 (BFD MAD VLAN).

   ```
   <Sysname> system-view
   [Sysname] vlan 1000
   ```

   # Add all ports used for BFD MAD to the VLAN, including Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 2/0/1, Ten-GigabitEthernet 3/0/1, and Ten-GigabitEthernet 4/0/1.

   ```
   [Sysname-vlan1000] port ten-gigabitethernet 1/0/1 ten-gigabitethernet 2/0/1
   ten-gigabitethernet 3/0/1 ten-gigabitethernet 4/0/1
   [Sysname-vlan3] quit
   ```

Create VLAN-interface 1000, and configure a MAD IP address for each member device on the interface.

```
[Sysname] interface vlan-interface 1000
[Sysname-Vlan-interface1000] mad bfd enable
[Sysname-Vlan-interface1000] mad ip address 192.168.2.1 24 member 1
[Sysname-Vlan-interface1000] mad ip address 192.168.2.2 24 member 2
[Sysname-Vlan-interface1000] mad ip address 192.168.2.3 24 member 3
[Sysname-Vlan-interface1000] mad ip address 192.168.2.4 24 member 4
[Sysname-Vlan-interface1000] quit
```

Disable the spanning tree feature on the ports in the BFD MAD VLAN.

```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo stp enable
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] interface ten-gigabitethernet 2/0/1
[Sysname-Ten-GigabitEthernet2/0/1] undo stp enable
[Sysname-Ten-GigabitEthernet2/0/1] quit
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] undo stp enable
[Sysname-Ten-GigabitEthernet3/0/1] quit
[Sysname] interface ten-gigabitethernet 4/0/1
[Sysname-Ten-GigabitEthernet4/0/1] undo stp enable
[Sysname-Ten-GigabitEthernet4/0/1] quit
```

2. Configure the access switch:

Create VLAN 1000 (BFD MAD VLAN).

```
<Sysname> system-view
[Sysname] vlan 1000
```

Add all ports used for BFD MAD to the VLAN, including GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4.

```
[Sysname-vlan1000] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet
1/0/3 gigabitethernet 1/0/4
[Sysname-vlan3] 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 physical ports to the aggregation group for Bridge-Aggregation 40. These physical ports are Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 1/0/2, Ten-GigabitEthernet 1/0/3, and Ten-GigabitEthernet 1/0/4.

```
[RouterA] interface ten-gigabitethernet 1/0/1
[RouterA-Ten-GigabitEthernet1/0/1] port link-aggregation group 40
[RouterA-Ten-GigabitEthernet1/0/1] quit
[RouterA] interface ten-gigabitethernet 1/0/2
[RouterA-Ten-GigabitEthernet1/0/2] port link-aggregation group 40
[RouterA-Ten-GigabitEthernet1/0/2] quit
[RouterA] interface ten-gigabitethernet 1/0/3
[RouterA-Ten-GigabitEthernet1/0/3] port link-aggregation group 40
[RouterA-Ten-GigabitEthernet1/0/3] quit
[RouterA] interface ten-gigabitethernet 1/0/4
[RouterA-Ten-GigabitEthernet1/0/4] port link-aggregation group 40
[RouterA-Ten-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 Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 to the aggregation group for Bridge-Aggregation 42.

```
[RouterA] interface ten-gigabitethernet 1/0/5
[RouterA-Ten-GigabitEthernet1/0/5] port link-aggregation group 42
[RouterA-Ten-GigabitEthernet1/0/5] quit
[RouterA] interface ten-gigabitethernet 1/0/6
[RouterA-Ten-GigabitEthernet1/0/6] port link-aggregation group 42
[RouterA-Ten-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 to 42
```

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 physical ports to the aggregation group for Bridge-Aggregation 41. These physical ports are Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 1/0/2, Ten-GigabitEthernet1/0/3, and Ten-GigabitEthernet 1/0/4.

```
[RouterB] interface ten-gigabitethernet 1/0/1
[RouterB-Ten-GigabitEthernet1/0/1] port link-aggregation group 41
[RouterB-Ten-GigabitEthernet1/0/1] quit
[RouterB] interface ten-gigabitethernet 1/0/2
[RouterB-Ten-GigabitEthernet1/0/2] port link-aggregation group 41
[RouterB-Ten-GigabitEthernet1/0/2] quit
[RouterB] interface ten-gigabitethernet 1/0/3
[RouterB-Ten-GigabitEthernet1/0/3] port link-aggregation group 41
[RouterB-Ten-GigabitEthernet1/0/3] quit
[RouterB] interface ten-gigabitethernet 1/0/4
[RouterB-Ten-GigabitEthernet1/0/4] port link-aggregation group 41
[RouterB-Ten-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 Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 to the aggregation group for Bridge-Aggregation 42.

```
[RouterB] interface ten-gigabitethernet 1/0/5
[RouterB-Ten-GigabitEthernet1/0/5] port link-aggregation group 42
[RouterB-Ten-GigabitEthernet1/0/5] quit
[RouterB] interface ten-gigabitethernet 1/0/6
[RouterB-Ten-GigabitEthernet1/0/6] port link-aggregation group 42
[RouterB-Ten-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, 40, and 41.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] vlan 20
[Sysname-vlan20] 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 physical ports to the aggregation group for Bridge-Aggregation 10. These physical ports are Ten-GigabitEthernet 1/0/10, Ten-GigabitEthernet 2/0/10, Ten-GigabitEthernet 3/0/10, and Ten-GigabitEthernet 4/0/10.

```
[Sysname] interface ten-gigabitethernet 1/0/10
[Sysname-Ten-GigabitEthernet1/0/10] port link-aggregation group 10
[Sysname-Ten-GigabitEthernet1/0/10] quit
[Sysname] interface ten-gigabitethernet 2/0/10
[Sysname-Ten-GigabitEthernet2/0/10] port link-aggregation group 10
[Sysname-Ten-GigabitEthernet2/0/10] quit
[Sysname] interface ten-gigabitethernet 3/0/10
[Sysname-Ten-GigabitEthernet3/0/10] port link-aggregation group 10
[Sysname-Ten-GigabitEthernet3/0/10] quit
[Sysname] interface ten-gigabitethernet 4/0/10
[Sysname-Ten-GigabitEthernet4/0/10] port link-aggregation group 10
[Sysname-Ten-GigabitEthernet4/0/10] 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 Bridge-Aggregation 10 configuration steps to configure Bridge-Aggregation interfaces 20, 40, and 41, in compliance with the scheme in Table 13. (Details not shown.)

Create interfaces for VLANs 10, 20, 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 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 10.214.50.0 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 physical ports to the aggregation group for Bridge-Aggregation 10. These physical ports are Ten-GigabitEthernet 1/0/49, Ten-GigabitEthernet 1/0/50, Ten-GigabitEthernet 1/0/51, and Ten-GigabitEthernet 1/0/52.

```
[DeviceE] interface ten-gigabitethernet 1/0/49
[DeviceE-Ten-GigabitEthernet1/0/49] port link-aggregation group 10
[DeviceE-Ten-GigabitEthernet1/0/49] quit
[DeviceE] interface ten-gigabitethernet 1/0/50
[DeviceE-Ten-GigabitEthernet1/0/50] port link-aggregation group 10
[DeviceE-Ten-GigabitEthernet1/0/50] quit
[DeviceE] interface ten-gigabitethernet 1/0/51
[DeviceE-Ten-GigabitEthernet1/0/51] port link-aggregation group 10
[DeviceE-Ten-GigabitEthernet1/0/51] quit
[DeviceE] interface ten-gigabitethernet 1/0/52
```

```
[DeviceE-Ten-GigabitEthernet1/0/52] port link-aggregation group 10
[DeviceE-Ten-GigabitEthernet1/0/52] quit
```

5. Configure Device F and Device G in the same way you configure Device E, in compliance with Table 13. (Details not shown.)

Verifying the configuration

Verify the IRF setup, routing configuration, multichassis link aggregations, ring topology, and BFD MAD.

Verifying the IRF setup

Execute the **display irf** command to verify that the IRF fabric has been formed.

```
[Sysname] display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  31        0cda-414a-859c  ---
   2        Standby 1         00a0-fc00-5801  ---
   3        Standby 1         0cda-415e-232f  ---
   4        Standby 1         00e0-fc58-1235  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0cda-414a-859b
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 2
```

The output shows that the IRF fabric has four member devices.

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         2             UP         4           0cda-414a-859b
 2           UP         3             UP         1           0cda-414a-859b
 3           UP         4             UP         2           0cda-414a-859b
 4           UP         1             UP         3           0cda-414a-859b
```

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 : 13       Routes : 13

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
10.214.50.0/30          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 Ten-GigabitEthernet 1/0/13, a member port of Bridge-Aggregation 40.

```
[Sysname] interface ten-gigabitethernet 1/0/13
[Sysname-Ten-GigabitEthernet1/0/13] shutdown
[Sysname-Ten-GigabitEthernet1/0/13] 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=8ms TTL=127
Reply from 10.214.50.2: bytes=32 time=7ms TTL=127
Reply from 10.214.50.2: bytes=32 time=2ms TTL=127
Reply from 10.214.50.2: bytes=32 time=278ms TTL=127
Reply from 10.214.50.2: bytes=32 time=7ms TTL=127
```

The output shows that the address can be pinged after a short delay.

Verifying link failure protection of the ring topology

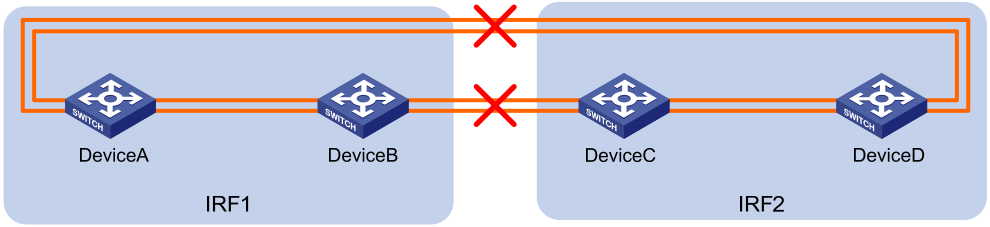
Disconnect all IRF links between two IRF member devices. (Details not shown.)

Verify that the IRF fabric can operate correctly as a daisy chained fabric. (Details not shown.)

Verifying the BFD MAD configuration

Disconnect two IRF connections: one between Device A and Device D, and the other between Device B and Device C. The disconnect actions cause the IRF fabric to break down into two parts: IRF 1 (Device A and Device B) and IRF 2 (Device C and Device D). See Figure 105.

Figure 105 IRF split



Verify that BFD MAD detects the split and displays IRF link state and member device failure messages. The following is the sample output from IRF 1:

```
%Jan  1 05:19:10:176 2011 HP STM/3/STM_LINK_STATUS_DOWN: IRF port 2 is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/27 link status
is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/28 link status
is down.
%Jan  1 05:19:10:176 2011 HP STM/3/STM_LINK_STATUS_DOWN: IRF port 1 is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet2/0/25 link status
is down.
%Jan  1 05:19:10:184 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet2/0/26 link status
is down.
%Jan  1 05:19:10:186 2011 HP DEV/3/BOARD_REMOVED: Board is removed from Slot 3, type is
MAIN_BOARD_TYPE_52QF.
%Jan  1 05:19:10:186 2011 HP DEV/3/BOARD_REMOVED: Board is removed from Slot 4, type is
MAIN_BOARD_TYPE_52QF.
%Jan   1  00:40:22:534  2011  HP  BFD/5/BFD_CHANGE_FSM:  Sess[192.168.2.1/192.168.2.3,
LD/RD:33/33, Interface:Vlan1000, SessType:Ctrl, LinkType:INET], Sta: DOWN->INIT, Diag:
0
%Jan   1  00:40:22:791  2011  HP  BFD/5/BFD_CHANGE_FSM:  Sess[192.168.2.1/192.168.2.3,
LD/RD:33/33, Interface:Vlan1000, SessType:Ctrl, LinkType:INET], Sta: INIT->UP, Diag: 0
%Jan  1 00:40:27:962 2011 HP BFD/5/BFD_CHANGE_FSM: Sess[192.168.2.1/192.168.2.3,
LD/RD:33/33, Interface:Vlan1000, SessType:Ctrl, LinkType:INET], Sta: UP->DOWN, Diag: 1
```

The output shows that the BFD session was up for a short time after the IRF split. Because the master device in IRF 1 has a lower member ID than the master device in IRF 2, BFD MAD then changed IRF 2 (Device C and Device D) to the Recovery state. The BFD session was down after BFD MAD shut down all physical network ports on Device C and Device D, except for the IRF physical ports and ports configured to be excluded from the shutdown action.

Log in to IRF 2, and verify that the IRF fabric is in Recovery state.

```
<Sysname> display mad verbose
Current MAD status: Recovery
Excluded ports(configurable):
Excluded ports(can not be configured):
  Ten-GigabitEthernet3/0/45
  Ten-GigabitEthernet3/0/46
  Ten-GigabitEthernet3/0/47
  Ten-GigabitEthernet3/0/48
  Ten-GigabitEthernet4/0/45
  Ten-GigabitEthernet4/0/46
  Ten-GigabitEthernet4/0/47
  Ten-GigabitEthernet4/0/48
```

```
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface:
  Vlan-interface1000
    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
```

Recover the IRF links. The following message is displayed:

```
%Jan  1 00:52:25:555 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/28 link status
is up.
%Jan  1 00:52:25:555 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/28 is up.
%Jan  1 00:52:25:717 2011 HP STM/6/STM_LINK_STATUS_UP: IRF port 2 is up.
%Jan  1 00:52:26:257 2011 HP STM/4/STM_LINK_RECOVERY: Merge occurs.
%Jan  1 00:52:30:834 2011 HP STM/3/STM_LINK_STATUS_DOWN: IRF port 2 is down.
%Jan  1 00:52:30:835 2011 HP IFNET/3/PHY_UPDOWN: Ten-GigabitEthernet1/0/28 link status
is down.
%Jan  1 00:52:30:836 2011 HP IFNET/5/LINK_UPDOWN: Line protocol on the interface
Ten-GigabitEthernet1/0/28 is down.
```

IRF 2 reboots automatically to merge with IRF 1.

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         2             UP         4           0cda-414a-859b
 2           UP         3             UP         1           0cda-414a-859b
 3           UP         4             UP         2           0cda-414a-859b
 4           UP         1             UP         3           0cda-414a-859b
```

Configuration files

- IRF fabric:

```
#
vlan 10
#
vlan 20
#
vlan 40
#
vlan 41
#
vlan 1000
#
irf-port 1/1
```

```
 port group interface Ten-GigabitEthernet1/0/25
 port group interface Ten-GigabitEthernet1/0/26
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/0/27
 port group interface Ten-GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/0/25
 port group interface Ten-GigabitEthernet2/0/26
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/27
 port group interface Ten-GigabitEthernet2/0/28
#
irf-port 3/1
 port group interface Ten-GigabitEthernet3/0/25
 port group interface Ten-GigabitEthernet3/0/26
#
irf-port 3/2
 port group interface Ten-GigabitEthernet3/0/27
 port group interface Ten-GigabitEthernet3/0/28
#
irf-port 4/1
 port group interface Ten-GigabitEthernet4/0/25
 port group interface Ten-GigabitEthernet4/0/26
#
irf-port 4/2
 port group interface Ten-GigabitEthernet4/0/27
 port group interface Ten-GigabitEthernet4/0/28
#
interface Bridge-Aggregation10
 port access vlan 10
 link-aggregation mode dynamic
#
interface Bridge-Aggregation20
 port access vlan 20
 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-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-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 Vlan-interface1000
 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 Te-Gigabitethernet 1/0/1
 port link-mode bridge
 stp disable
 port access vlan 1000
#
interface Ten-Gigabitethernet 1/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface Ten-Gigabitethernet 1/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface Ten-Gigabitethernet 1/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface Ten-Gigabitethernet 1/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface Ten-Gigabitethernet 2/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
```

```
interface Ten-Gigabitethernet 2/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface Ten-Gigabitethernet 2/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface Ten-Gigabitethernet 2/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface Ten-Gigabitethernet 3/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface Ten-Gigabitethernet 3/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface Ten-Gigabitethernet 3/0/13
 port link-mode bridge
 port access vlan 40
 port link-aggregation group 40
#
interface Ten-Gigabitethernet 3/0/14
 port link-mode bridge
 port access vlan 41
 port link-aggregation group 41
#
interface Ten-Gigabitethernet 4/0/10
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 10
#
interface Ten-Gigabitethernet 4/0/11
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 20
#
interface Ten-Gigabitethernet 4/0/13
 port link-mode bridge
 port access vlan 40
```

```
 port link-aggregation group 40
#
interface Ten-Gigabitethernet 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 10.214.50.0 0.0.0.3
  network 10.214.50.4 0.0.0.3
```

- 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
```

IS-IS configuration examples

This chapter provides IS-IS configuration examples.

Example: Configuring basic IS-IS

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

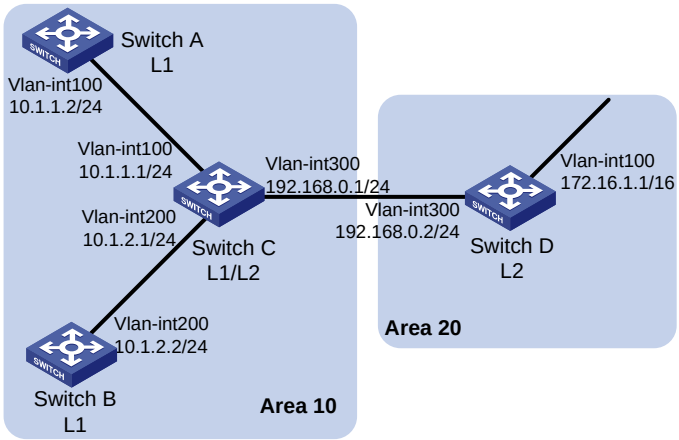
Network requirements

As shown in Figure 106, Switch A, Switch B, Switch C, and Switch D reside in an IS-IS AS.

Switch A and B are Level-1 switches, Switch D is a Level-2 switch, and Switch C is a Level-1-2 switch. Switch A, Switch B, and Switch C are in Area 10, and Switch D is in Area 20.

Configure basic IS-IS functions to enable the communication in the AS.

Figure 106 Network requirements



Configuration procedures

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IS-IS:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
```

```
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[SwitchB-Vlan-interface200] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
```

Configure Switch D.

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 100
[SwitchD-Vlan-interface100] isis enable 1
[SwitchD-Vlan-interface100] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit
```

Verifying the configuration

Display IS-IS neighbor information for each switch.

```
[SwitchA]display isis peer

                    Peer information for IS-IS(1)
```

```
                        ----------------------------

 System Id: 0000.0000.0003
 Interface: Vlan100                Circuit Id:  0000.0000.0001.01
 State: Up     HoldTime:  24s       Type: L1(L1L2)     PRI: 64

[SwitchB]display isis peer

                        Peer information for IS-IS(1)
                        ----------------------------

 System Id: 0000.0000.0003
 Interface: Vlan100                Circuit Id:  0000.0000.0002.01
 State: Up     HoldTime:  24s       Type: L1(L1L2)     PRI: 64

 [SwitchC]display isis peer

                        Peer information for IS-IS(1)
                        ----------------------------

 System Id: 0000.0000.0001
 Interface: Vlan100                Circuit Id:  0000.0000.0001.01
 State: Up     HoldTime:   7s       Type: L1           PRI: 64

 System Id: 0000.0000.0004
 Interface: Vlan300                Circuit Id:  0000.0000.0004.01
 State: Up     HoldTime:   8s       Type: L2           PRI: 64

 System Id: 0000.0000.0002
 Interface: Vlan200                Circuit Id:  0000.0000.0002.01
 State: Up     HoldTime:   8s       Type: L1           PRI: 64

[SwitchD]display isis peer

                        Peer information for IS-IS(1)
                        ----------------------------

 System Id: 0000.0000.0003
 Interface: Vlan300                Circuit Id:  0000.0000.0004.01
 State: Up     HoldTime:  24s       Type: L2(L1L2)     PRI: 64
```

The output shows that Switch C becomes the neighbor of Switch A, Switch B, and Switch D.

Display the IS-IS LSDB on each switch to verify the LSPs.

```
[SwitchA] display isis lsdb

                       Database information for IS-IS(1)
                       --------------------------------

                          Level-1 Link State Database
```

```
                          --------------------------

LSPID                 Seq Num      Checksum   Holdtime   Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x00000004   0xdf5e     1096       68      0/0/0
0000.0000.0002.00-00  0x00000004   0xee4d     1102       68      0/0/0
0000.0000.0002.01-00  0x00000001   0xdaaf     1102       55      0/0/0
0000.0000.0003.00-00  0x00000009   0xcaa3     1161       111     1/0/0
0000.0000.0003.01-00  0x00000001   0xadda     1112       55      0/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
[SwitchB] display isis lsdb

                       Database information for IS-IS(1)
                       ---------------------------------

                          Level-1 Link State Database
                          --------------------------

LSPID                 Seq Num      Checksum   Holdtime    Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xdb60     988         68      0/0/0
0000.0000.0002.00-00* 0x00000008   0xe651     1189        68      0/0/0
0000.0000.0002.01-00* 0x00000005   0xd2b3     1188        55      0/0/0
0000.0000.0003.00-00  0x00000014   0x194a     1190        111     1/0/0
0000.0000.0003.01-00  0x00000002   0xabdb     995         55      0/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
[SwitchC] display isis lsdb

                       Database information for IS-IS(1)
                       ---------------------------------

                          Level-1 Link State Database
                          --------------------------

LSPID                 Seq Num      Checksum   Holdtime    Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000006   0xdb60     847         68      0/0/0
0000.0000.0002.00-00  0x00000008   0xe651     1053        68      0/0/0
0000.0000.0002.01-00  0x00000005   0xd2b3     1052        55      0/0/0
0000.0000.0003.00-00* 0x00000014   0x194a     1051        111     1/0/0
0000.0000.0003.01-00* 0x00000002   0xabdb     854         55      0/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

                          Level-2 Link State Database
                          --------------------------
```

```
LSPID                 Seq Num      Checksum   Holdtime    Length  ATT/P/OL
---------------------------------------------------------------------------
0000.0000.0003.00-00* 0x00000012   0xc93c     842         100     0/0/0
0000.0000.0004.00-00  0x00000026   0x331      1173        84      0/0/0
0000.0000.0004.01-00  0x00000001   0xee95     668         55      0/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
[SwitchD] display isis lsdb

                        Database information for IS-IS(1)
                        ---------------------------------

                           Level-2 Link State Database
                           ---------------------------

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0003.00-00  0x00000013   0xc73d        1003          100     0/0/0
0000.0000.0004.00-00* 0x0000003c   0xd647        1194          84      0/0/0
0000.0000.0004.01-00* 0x00000002   0xec96        1007          55      0/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Display the IS-IS routing information on each switch.

```
[SwitchA] display isis route

                          Route information for IS-IS(1)
                          ------------------------------

                          Level-1 IPv4 Forwarding Table
                          -----------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 10.1.1.0/24          10         NULL    Vlan100         Direct          D/L/-
 10.1.2.0/24          20         NULL    Vlan100         10.1.1.1        R/-/-
 192.168.0.0/24       20         NULL    Vlan100         10.1.1.1        R/-/-
 0.0.0.0/0            10         NULL    Vlan100         10.1.1.1        R/-/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
[SwitchC] display isis route

                          Route information for IS-IS(1)
                          ------------------------------

                          Level-1 IPv4 Forwarding Table
                          -----------------------------
```

```
 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 192.168.0.0/24       10         NULL    Vlan300         Direct          D/L/-
 10.1.1.0/24          10         NULL    Vlan100         Direct          D/L/-
 10.1.2.0/24          10         NULL    Vlan200         Direct          D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

                        Level-2 IPv4 Forwarding Table
                        -----------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 192.168.0.0/24       10         NULL    Vlan300         Direct          D/L/-
 10.1.1.0/24          10         NULL    Vlan100         Direct          D/L/-
 10.1.2.0/24          10         NULL    Vlan200         Direct          D/L/-
 172.16.0.0/16        20         NULL    Vlan300         192.168.0.2     R/-/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
[SwitchD] display isis route

                        Route information for IS-IS(1)
                        ------------------------------

                        Level-2 IPv4 Forwarding Table
                        -----------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 192.168.0.0/24       10         NULL    Vlan300         Direct          D/L/-
 10.1.1.0/24          20         NULL    Vlan300         192.168.0.1     R/-/-
 10.1.2.0/24          20         NULL    Vlan300         192.168.0.1     R/-/-
 172.16.0.0/16        10         NULL    Vlan100         Direct          D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

The output shows that the routing table of Level-1 switches contains a default route with the next hop as the Level-1-2 switch. The routing table of the Level-2 switch contains routing information of Level-1 and Level-2.

Configuration files

- Switch A:

```
#
isis 1
is-level level-1
network-entity 10.0000.0000.0001.00
#
vlan 100
```

```
#
interface Vlan-interface100
ip address 10.1.1.2 255.255.255.0
isis enable 1
#
```

- Switch B:

```
#
isis 1
is-level level-1
network-entity 10.0000.0000.0002.00
#
vlan 200
#
interface Vlan-interface200
ip address 10.1.2.2 255.255.255.0
isis enable 1
#
```

- Switch C:

```
#
isis 1
network-entity 10.0000.0000.0003.00
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
isis enable 1
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
isis enable 1
#
interface Vlan-interface300
 ip address 192.168.0.1 255.255.255.0
isis enable 1
```

- Switch D:

```
#
isis 1
network-entity 10.0000.0000.0004.00
is-level level-2
#
vlan 100
#
vlan 300
```

```
#
interface Vlan-interface100
ip address 172.16.1.1 255.255.0.0
isis enable 1
#
interface Vlan-interface300
ip address 192.168.0.2 255.255.255.0
isis enable 1
#
```

Example: Configuring IS-IS GR

Applicable product matrix

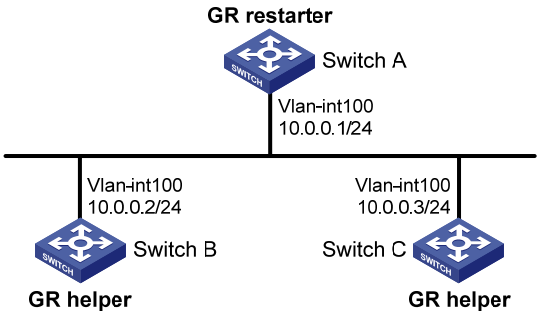
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 107, Switch A, Switch B, and Switch C belong to the same IS-IS routing domain.

Configure IS-IS GR to avoid communication interruption during the protocol restart period on Switch A.

Figure 107 Network diagram



Configuration procedures

1. Configure IP addresses and subnet masks for interfaces. (Details not shown.)
2. Configure IS-IS on the switches to make sure Switch A, Switch B, and Switch C can communicate with each other at Layer 3and dynamic route update can be implemented among them with IS-IS. (Details not shown.)
3. Configure IS-IS GR:

   # Enable IS-IS GR on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] isis 1
   ```

```
[SwitchA-isis-1] graceful-restart
[SwitchA-isis-1] return
```

Verifying the configuration

During the GR period, route entries on the switches are intact, and the communication between the switches is not interrupted. You can verify the network connectivity by using the **ping** command.

Restart the IS-IS process on Switch A.

```
<SwitchA> reset isis all 1 graceful-restart
Reset IS-IS process? [Y/N]:y
```

Check the GR status of IS-IS on Switch A.

```
<SwitchA> display isis graceful-restart status

                      Restart information for IS-IS(1)
                      --------------------------------
Restart status: COMPLETE
Restart phase: Finish
Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
SA Bit: supported

                        Level-1 restart information
                        ---------------------------
Total number of interfaces: 1
Number of waiting LSPs: 0

                        Level-2 restart information
                        ---------------------------
Total number of interfaces: 1
Number of waiting LSPs: 0
```

Configuration files

- Switch A:

```
#
isis 1
is-level level-1
graceful-restart
network-entity 10.0000.0000.0001.00
#
vlan 100
#
interface Vlan-interface100
ip address 10.0.0.1 255.255.255.0
isis enable 1
#
```

- Switch B:

```
#
```

```
isis 1
is-level level-1
network-entity 10.0000.0000.0002.00
#
vlan 100
#
interface Vlan-interface100
ip address 10.0.0.2 255.255.255.0
isis enable 1
#
```

- Switch C:

```
#
isis 1
is-level level-1
network-entity 10.0000.0000.0003.00
#
vlan 100
#
interface Vlan-interface100
ip address 10.1.1.2 255.255.255.0
isis enable 1
#
```

Example: Configuring BFD for IS-IS

Applicable product matrix

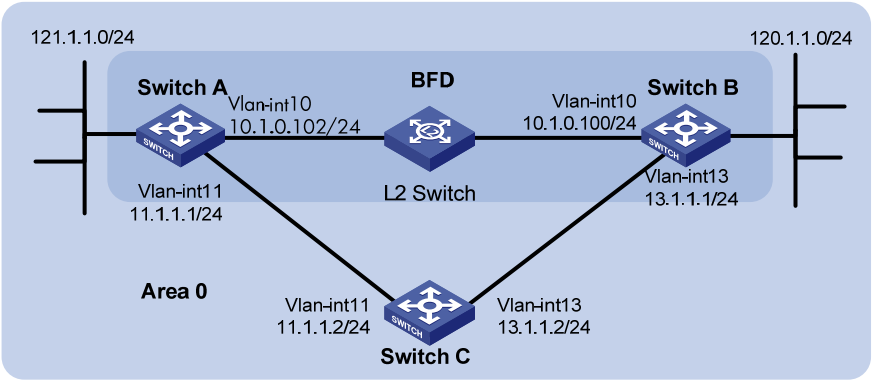
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 108, run IS-IS on Switch A, Switch B, and Switch C so that they can reach each other at the network layer.

After the link over which Switch A and Switch B communicate through the Layer 2 switch fails, BFD can quickly detect the failure and notify IS-IS of the failure. Switch A and Switch B then communicate through Switch C.

Figure 108 Network diagram



Configuration restrictions and guidelines

To configure BFD control packet mode for IS-IS, you must enable BFD on both ends of the BFD session.

Configuration procedures

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic IS-IS:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] isis
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] isis enable
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] isis enable
[SwitchA-Vlan-interface11] quit
```

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] isis
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] isis enable
[SwitchB-Vlan-interface10] quit
[SwitchB] interface vlan-interface 13
[SwitchB-Vlan-interface13] isis enable
[SwitchB-Vlan-interface13] quit
```

   # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] isis
```

```
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 11
[SwitchC-Vlan-interface11] isis enable
[SwitchC-Vlan-interface11] quit
[SwitchC] interface vlan-interface 13
[SwitchC-Vlan-interface13] isis enable
[SwitchC-Vlan-interface13] quit
```

3. Configure BFD functions:

Enable BFD on Switch A.

```
[SwitchA] bfd session init-mode passive
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] isis bfd enable
```

Enable BFD on Switch B.

```
[SwitchB] bfd session init-mode active
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] isis bfd enable
```

Verifying the configuration

Display the BFD session information on Switch A.

```
<SwitchA> display bfd session

Total Session Num: 1     Up Session Num: 1     Init Mode: Passive

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 33/33          10.1.0.102      10.1.0.100      Up       3820ms
```

Display routes destined for 120.1.1.0/24 on Switch A.

```
<SwitchA> display ip routing-table 120.1.1.0 verbose

Summary Count : 1

Destination: 120.1.1.0/24
   Protocol: ISIS            Process ID: 1
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 10              Preference: 10
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 10.1.0.100
      Label: NULL           RealNextHop: 10.1.0.100
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: Vlan-interface10
```

```
BkTunnel ID: Invalid        BkInterface: N/A
```

The output shows that Switch A and Switch B communicate through L2 Switch. Then the link over L2 Switch fails.

Display routes destined for 120.1.1.0/24 on Switch A.

```
<SwitchA> display ip routing-table 120.1.1.0 verbose

Summary Count : 1

Destination: 120.1.1.0/24
   Protocol: ISIS            Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 20              Preference: 10
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NBRID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 11.1.1.2
      Label: NULL            RealNextHop: 11.1.1.2
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
```

The output shows that Switch A and Switch B communicate through Switch C.

Configuration files

- Switch A:

```
#
isis
network-entity 10.0000.0000.0001.00
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
 isis bfd enable
isis enable 1
#
vlan 11
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
isis enable 1
#
vlan 12
#
interface Vlan-interface12
```

```
 ip address 121.1.1.1 255.255.255.0
isis enable 1
#
bfd session init-mode passive
#
```

- Switch B:

```
#
isis
network-entity 10.0000.0000.0002.00
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.0.100 255.255.255.0
 isis bfd enable
isis enable 1
#
vlan 12
#
interface Vlan-interface12
 ip address 120.1.1.1 255.255.255.0
isis enable 1
#
vlan 13
#
interface Vlan-interface13
 ip address 13.1.1.1 255.255.255.0
isis enable 1
#
bfd session init-mode active
#
```

- Switch C:

```
#
isis
network-entity 10.0000.0000.0003.00
#
vlan 11
#
interface Vlan-interface11
 ip address 11.1.1.2 255.255.255.0
isis enable 1
#
vlan 13
#
interface Vlan-interface13
 ip address 13.1.1.2 255.255.255.0
isis enable 1
#
```

ISSU examples

This chapter provides examples for using ISSU to upgrade the switch.

ISSU has a series of **install** commands and a series of **issu** commands. These two series of commands support different upgrade types, as shown in Table 14.

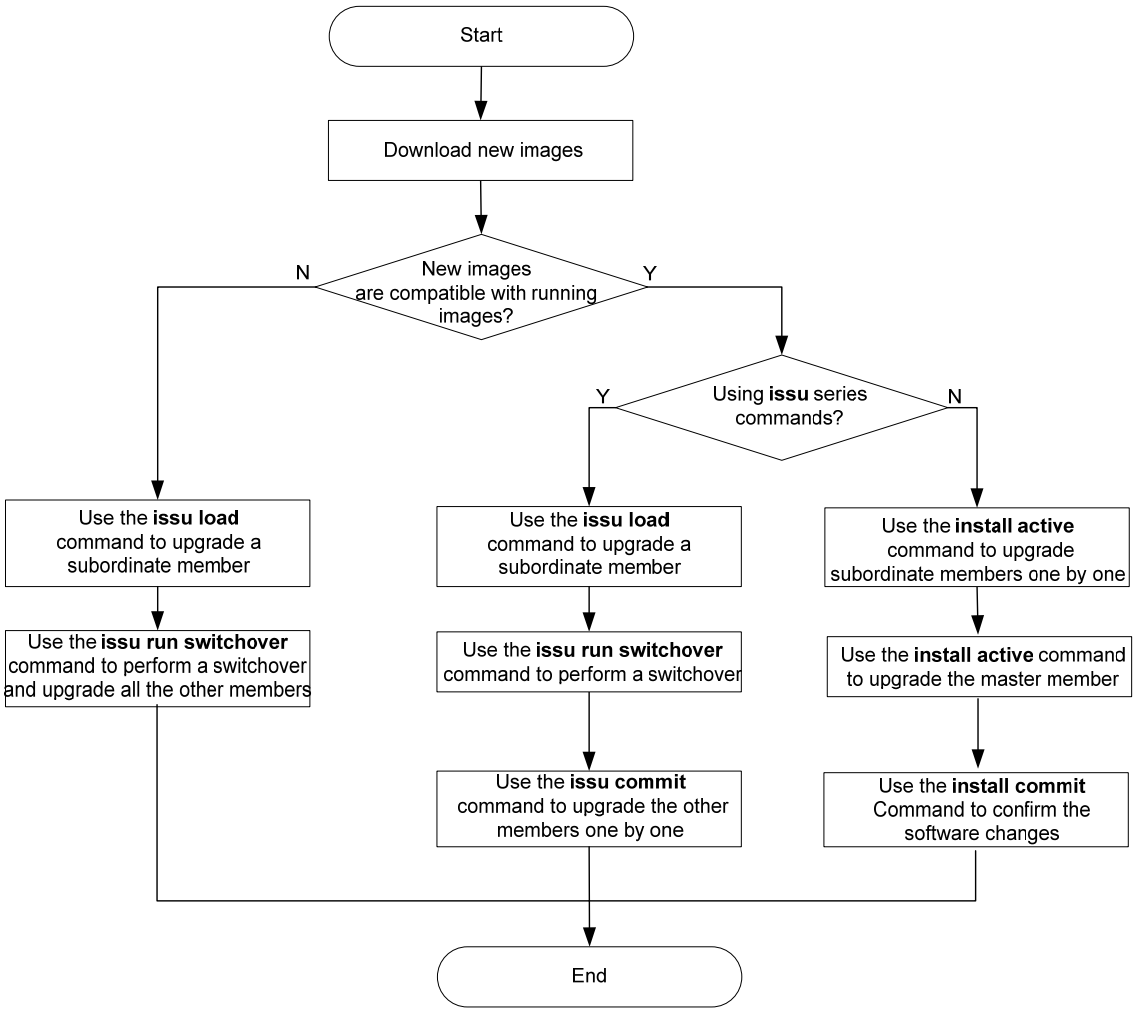
Table 14 Command series and upgrade types

Upgrade type	issu commands	install commands
Upgrade to a compatible version:		
Incremental upgrade	Yes	Yes
ISSU reboot upgrade	Yes	Yes
Reboot upgrade	Yes	Yes
Upgrade to an incompatible version	Yes	No
Installing and uninstalling patches	No	Yes

Before an ISSU, use the **display version comp-matrix** command to display the compatibility between the running images and the new images and identify the recommended ISSU method. The key to a successful ISSU is to use the recommended method and follow the correct procedure for the method.

Figure 109 shows the ISSU procedures for ISSU methods.

Figure 109 ISSU procedures for ISSU methods



Example: Performing a reboot upgrade to a compatible version by using issu commands

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

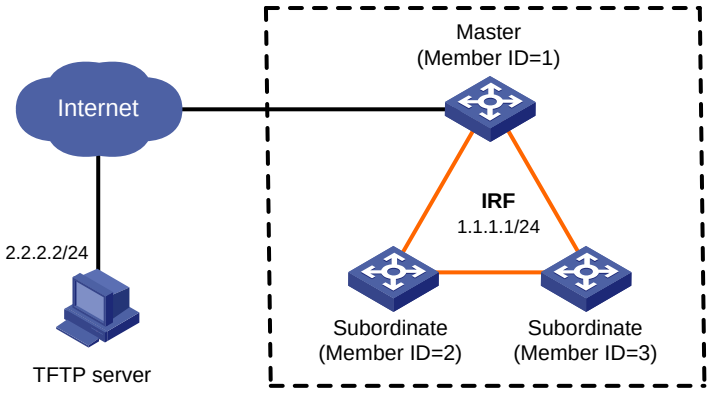
Network requirements

As shown in Figure 110, the IRF fabric has three members, and IRF member 1 is the master.

- Use **issu** commands to perform a reboot upgrade for the IRF fabric.

- Set the automatic rollback timer to roll back the upgrade if the timer is not deleted before the timer expires.

Figure 110 Network diagram



Note: The orange links are IRF links.

Upgrade restrictions and guidelines

When you perform an ISSU, follow these restrictions and guidelines:

- Before the upgrade, make sure each IRF member's flash memory has free space that is at least twice the image file size.
- During the upgrade, make sure the following requirements are met:
  - Do not execute any commands that are not for the ISSU.
  - Prevent other operators from operating the device.

Upgrade procedures

Download the image file from the TFTP server to the root directory of the master's flash memory.

```
<Sysname> tftp 2.2.2.2 get example.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                 Dload  Upload   Total   Spent    Left  Speed
100 42.8M  100 42.8M    0     0   159k      0  0:04:34  0:04:34 --:--:--  165k
```

Display the current active software images on the IRF members.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 2:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 3:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
```

Identify the recommended ISSU method and its possible impacts on the device.

```
<Sysname> display version comp-matrix file ipe flash:/example.ipe
```

```
Boot image: boot-r2211.bin
  Version:
  7.1.035P11

System image: system-r2211.bin
  Version:
  R2211
  Version compatibility list:
  E2206P02
  R2207
  R2208
  R2208P01
  F2209
  R2209
  F2210
  R2210
  R2211
  R2211
  Version dependency boot list:
  7.1.035P11

  Slot  Upgrade Way
  1     Reboot
  2     Reboot
  3     Reboot
```

The output shows the following information:

- The two versions are compatible.
- Reboot upgrade is recommended.
- The IRF members will be rebooted during the upgrade.

Set the automatic rollback timer to 30 seconds.

```
<Sysname> system-view
[Sysname] issu rollback-timer 30
<Sysname> quit
```

Upgrade IRF member 2.

```
<Sysname> issu load file ipe flash:/example.ipe slot 2
This operation will delete the rollback point information for the previous upgrade
 and maybe get unsaved configuration lost. Continue? [Y/N]:y
Successfully copied flash:/boot-r2211.bin to slot2#flash:/boot-r2211.bin.
Successfully copied flash:/system-r2211.bin to slot2#flash:/system-r2211.bin.
Upgrade summary according to following table:

flash:/boot-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

flash:/system-r2211.bin
  Running Version             New Version
```

```
  Release 2210                Release 2211

  Slot  Upgrade Way
  2     Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

IRF member 2 reboots to complete the upgrade.

Verify that the upgrade has been completed on IRF member 2.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 2
Current upgrading slot: None
Current version list:
  boot: 7.1.035P11
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r2211.bin
  flash:/s5900_5920-cmw710-system-r2211.bin
```

After the upgrade is completed on the IRF member, the **ISSU state** field displays **Loaded**.

NOTE:

After you upgrade an IRF member, make sure the upgrade has been completed on the member before you continue with the following steps.

Perform a master/subordinate switchover.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/boot-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

flash:/system-r2210.bin
  Running Version             New Version
  Release 2210                Release 2211

  Slot  Switchover Way
  1     Master subordinate switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

IMPORTANT:

The **issu run switchover** command starts the automatic-rollback timer. To upgrade the IRF fabric successfully, you must execute the **issu accept** or **issu commit** command before the timer expires. If you fail to execute these commands before the timer expires, the system automatically rolls back to the original software images.

Verify that IRF member 2 has become the master.

```
<Sysname> display issu state
ISSU state: Switchover
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 2
Current upgrading slot: None
Current version list:
  boot: 7.1.035P11
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r2211.bin
  flash:/s5900_5920-cmw710-system-r2211.bin
```

After the switchover is completed, the **ISSU state** field displays **Switchover**.

Upgrade IRF member 1.

```
<Sysname> issu commit slot 1
Upgrade summary according to following table:

flash: /boot-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

flash: /boot-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

  Slot  Upgrade Way
  1     Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

IRF member 1 reboots to complete the upgrade.

NOTE:

The automatic-rollback timer is removed the first time you execute the **issu commit** command after you execute the **issu run switchover** command. You will not be able to use the ISSU rollback feature to roll back to the original software images.

Verify that the upgrade has been completed on IRF member 1.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 1
Current upgrading slot: None
Current version list:
  boot: 7.1.035P11
```

```
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r2211.bin
  flash:/s5900_5920-cmw710-system-r2211.bin
```

After the ISSU upgrade is completed on the IRF member, the **ISSU state** field displays **Loaded**.

Upgrade IRF member 3.

```
<Sysname> issu commit slot 3
Successfully copied flash:/boot-r2211.bin to slot3#flash:/boot-r2211.bin.
Successfully copied flash:/system-r2211.bin to slot3#flash:/system-r2211.bin.
Upgrade summary according to following table:

flash:/boot-r2210.bin
  Running Version             New Version
  Release 2210                Release 2211

flash:/system-r2210.bin
  Running Version             New Version
  Release 2210                Release 2211

  Slot  Upgrade Way
  3     Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

IRF member 3 reboots to complete the upgrade.

Verify that the upgrade has been completed on the IRF fabric.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 3
Current upgrading slot: None
Current version list:
  boot: 7.1.035P11
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r2211.bin
  flash:/s5900_5920-cmw710-system-r2211.bin
```

After the upgrade is completed for the entire IRF fabric, the **ISSU state** field displays **Init**.

Verifying the upgrade

Verify that the IRF members are running the new images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2211.bin
  flash:/system-r2211.bin
```

```
Active packages on slot 2:
  flash:/boot-r2211.bin
  flash:/system-r2211.bin
Active packages on slot 3:
  flash:/boot-r2211.bin
  flash:/system-r2211.bin
```

Configuration files

The system does not save the commands used in the procedures to a configuration file.

Example: Performing an ISSU reboot upgrade to a compatible version by using issu commands

Applicable product matrix

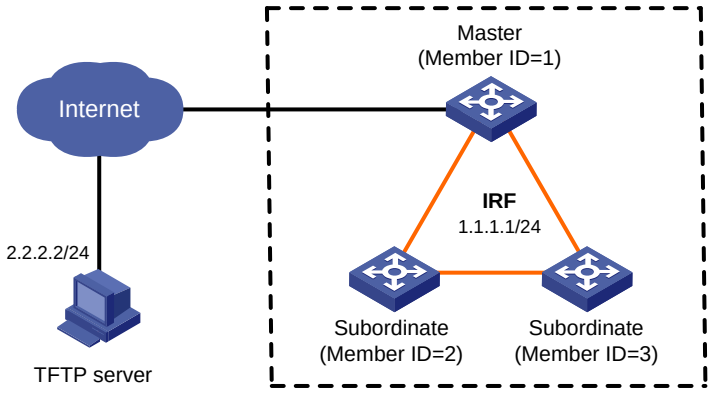
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 111, the IRF fabric has three members, and IRF member 1 is the master.

Use **issu** commands to perform an ISSU reboot upgrade for the IRF fabric. Set the automatic rollback timer to roll back the upgrade if the timer is not deleted before the timer expires.

Figure 111 Network diagram



Note: The orange links are IRF links.

Upgrade restrictions and guidelines

When you perform an ISSU, follow these restrictions and guidelines:

- Before the upgrade, make sure each IRF member's flash memory has free space that is at least twice the image file size.
- During the upgrade, make sure the following requirements are met:
  - Do not execute any commands that are not for the ISSU.
  - Prevent other operators from operating the device.

Upgrade procedures

Download the image file from the TFTP server to the root directory of the master's flash memory.

```
<Sysname> tftp 2.2.2.2 get example.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                 Dload  Upload   Total   Spent    Left  Speed
100 42.8M  100 42.8M    0     0   159k      0  0:04:34  0:04:34 --:--:--  165k
```

Display the current active software images on the IRF members.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 2:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 3:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
```

Identify the recommended ISSU method and its possible impacts on the device.

```
<Sysname> display version comp-matrix file ipe flash:/example.ipe
Boot image:boot-r22xx.bin
  Version:
  7.1.035P03

System image:system-r22xx.bin
  Version:
  R22xx
  Version compatibility list:
  E2206P02
  R2207
  R2208
  Version dependency boot list:
  7.1.035P02
  7.1.035P03

  Slot  Upgrade Way
  1     ISSU Reboot
  2     ISSU Reboot
  3     ISSU Reboot
```

The output shows the following information:

- The two versions are compatible.
- ISSU reboot upgrade is recommended.

Set the automatic rollback timer to 30 seconds.

```
<Sysname> system-view
[Sysname] issu rollback-timer 30
<Sysname> quit
```

Upgrade IRF member 2.

```
<Sysname> issu load file ipe flash:/example.ipe slot 2
This operation will delete the rollback point information for the previous upgrade
 and maybe get unsaved configuration lost. Continue? [Y/N]:y
The IRF members must be connected in a ring topology, please upgrade by other way.
 Continue? [Y/N]:y
Successfully copied flash:/boot-r22xx.bin to slot2#flash:/boot-r22xx.bin.
Successfully copied flash:/system-r22xx.bin to slot2#flash:/system-r22xx.bin.
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Upgrade Way
  1     ISSU Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

An ISSU reboot occurs on IRF member 2.

Verify that the upgrade has been completed on IRF member 2.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 2
Current upgrading slot: None
Current version list:
  boot: 7.1.035P03
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r22xx.bin
  flash:/s5900_5920-cmw710-system-r22xx.bin
```

After the upgrade is completed on the IRF member, the **ISSU state** field displays **Loaded**.

NOTE:

After you upgrade an IRF member, make sure the upgrade has been completed on the member before you continue with the following steps.

Perform a master/subordinate switchover.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Switchover Way
  1     Master subordinate switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

IMPORTANT:

The **issu run switchover** command starts the automatic-rollback timer. To upgrade the IRF fabric successfully, you must execute the **issu accept** or **issu commit** command before the timer expires. If you fail to execute these commands before the timer expires, the system automatically rolls back to the original software images.

Verify that IRF member 2 has become the master.

```
<Sysname> display issu state
ISSU state: Switchover
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 2
Current upgrading slot: None
Current version list:
  boot: 7.1.035P03
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r22xx.bin
  flash:/s5900_5920-cmw710-system-r22xx.bin
```

After the switchover is completed, the **ISSU state** field displays **Switchover**.

Upgrade IRF member 1.

```
<Sysname> issu commit slot 1
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
```

```
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Upgrade Way
  2     ISSU Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

An ISSU reboot occurs on IRF member 1.

Verify that the upgraded has been completed on IRF member 1.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 1
Current upgrading slot: None
Current version list:
  boot: 7.1.035P03
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r22xx.bin
  flash:/s5900_5920-cmw710-system-r22xx.bin
```

After the ISSU upgrade is completed on the IRF member, the **ISSU state** field displays **Loaded**.

Upgrade IRF member 3.

```
<Sysname> issu commit slot 3
Successfully copied flash:/boot-r22xx.bin to slot3#flash:/boot-r22xx.bin.
Successfully copied flash:/system-r22xx.bin to slot3#flash:/system-r22xx.bin.
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Upgrade Way
  3     ISSU Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

An ISSU reboot occurs on IRF member 3.

Verify that the upgrade has been completed on the IRF fabric.

```
<Sysname> display issu state
ISSU state: Loaded
```

```
Compatibility: Compatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 3
Current upgrading slot: None
Current version list:
  boot: 7.1.035P03
  system: Comware V700R001B35D604
Current software images:
  flash:/s5900_5920-cmw710-boot-r22xx.bin
  flash:/s5900_5920-cmw710-system-r22xx.bin
```

After the upgrade is completed for the entire IRF fabric, the **ISSU state** field displays **Init**.

Verifying the upgrade

Verify that the IRF members are running the new images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
Active packages on slot 2:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
Active packages on slot 3:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
```

Configuration files

The system does not save the commands used in the procedures to a configuration file.

Example: Performing an ISSU to a compatible version by using install commands

Applicable product matrix

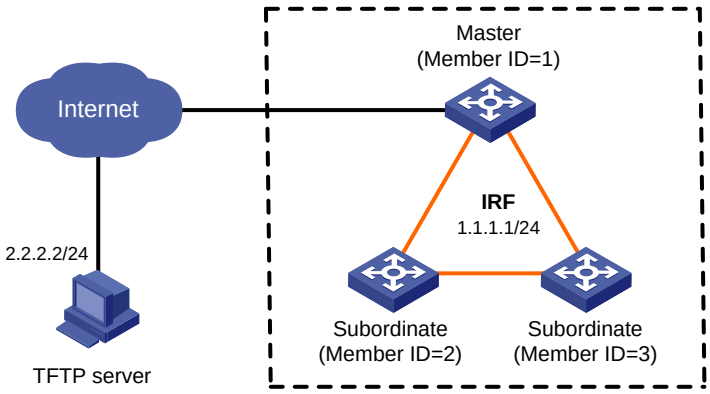
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 112, the IRF fabric has three members, and IRF member 1 is the master.

Use **install** commands to upgrade the IRF fabric to a compatible version.

Figure 112 Network diagram



Note: The orange links are IRF links.

Upgrade restrictions and guidelines

When you perform an ISSU, follow these restrictions and guidelines:

- Before the upgrade, make sure each IRF member's flash memory has free space that is at least twice the image file size.
- During the upgrade, make sure the following requirements are met:
  - Do not execute any commands that are not for the ISSU.
  - Prevent other operators from operating the device.

Upgrade procedures

Download the image file from the TFTP server to the root directory of the master's flash memory.

```
<Sysname> tftp 2.2.2.2 get example.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                 Dload  Upload   Total   Spent    Left  Speed
100 42.8M  100 42.8M    0     0   159k      0  0:04:34  0:04:34 --:--:--  165k
```

Decompress the file to the root directory of the master's flash memory.

```
<Sysname> install add flash:/example.ipe flash:
```

Display the current active software images on the IRF members.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 2:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 3:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
```

Identify the recommended ISSU method and its possible impacts on the device.

```
<Sysname> display version comp-matrix file ipe flash:/example.ipe
Boot image: boot-r22xx.bin
  Version:
  7.1.035P11

System image: system-r22xx.bin
  Version:
  R22xx
  Version compatibility list:
  E2206P02
  R2207
  R2208
  R2208P01
  F2209
  R2209
  F2210
  R2210
  R2211
  R2211
  Version dependency boot list:
  7.1.035P11

  Slot  Upgrade Way
  1     File Upgrade
  2     File Upgrade
  3     File Upgrade
```

The output shows the following information:

- The two versions are compatible.
- Incremental upgrade is recommended.

Upgrade IRF member 2.

```
<Sysname> install activate boot flash:/boot-r22xx.bin system
flash:/system-r22xx.bin slot 2
flash:/boot-r22xx.bin already exists on slot 2.
flash:/system-r22xx.bin already exists on slot 2.
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Upgrade Way
  2     File Upgrade
```

```
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

An incremental upgrade occurs on IRF member 2.

Verify that the upgrade has been completed on IRF member 2.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 2:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
Active packages on slot 3:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
```

After the upgrade is completed on the IRF member, the new images (flash:/boot-r22xx.bin and flash:/system-r22xx.bin) are displayed for the IRF member.

NOTE:

After you upgrade an IRF member, make sure the upgrade has been completed on the member before you continue with the following steps.

Upgrade IRF member 3.

```
<Sysname> install activate boot flash:/boot-r22xx.bin system
flash:/system-r22xx.bin slot 3
flash:/boot-r22xx.bin already exists on slot 3.
flash:/system-r22xx.bin already exists on slot 3.
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Upgrade Way
  3     File Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

An incremental upgrade occurs on IRF member 3.

Verify that the upgrade has been completed on IRF member 3.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 2:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
```

```
Active packages on slot 3:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
```

After the upgrade is completed on IRF member 3, the new images (flash:/boot-r22xx.bin and flash:/system-r22xx.bin in this example) are displayed for the IRF member.

Upgrade IRF member 1.

```
<Sysname> install activate boot flash:/boot-r22xx.bin system flash:/system-r22xx.bin slot
1
flash:/boot-r22xx.bin already exists on slot 1.
flash:/system-r22xx.bin already exists on slot 1.
Overwrite it?[Y/N]:y
Upgrade summary according to following table:

flash:/boot-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

flash:/system-r22xx.bin
  Running Version             New Version
  Release 2210                Release 22xx

  Slot  Upgrade Way
  1     File Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

Verify that the upgrade has been completed on IRF member 1.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
Active packages on slot 2:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
Active packages on slot 3:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
```

After the upgrade is completed on IRF member 1, the new images (flash:/boot-r22xx.bin and flash:/system-r22xx.bin in this example) are displayed for the IRF member.

Confirm the software changes to make them take effect after a reboot.

```
<Sysname> install commit
```

Verifying the upgrade

Verify that the IRF members are running the new images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
```

```
Active packages on slot 2:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
Active packages on slot 3:
  flash:/boot-r22xx.bin
  flash:/system-r22xx.bin
```

Configuration files

The system does not save the commands used in the procedures to a configuration file.

Example: Performing an ISSU to an incompatible version

Applicable product matrix

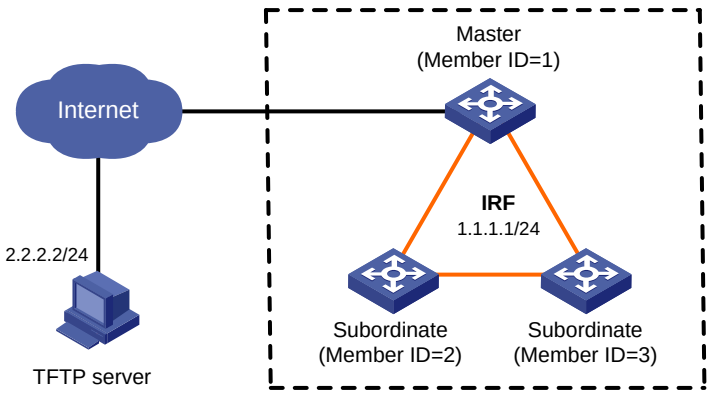
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 113, the IRF fabric has three members, and IRF member 1 is the master.

Upgrade the IRF fabric to an incompatible version.

Figure 113 Network diagram



Note: The orange links are IRF links.

Upgrade restrictions and guidelines

When you perform an ISSU, follow these restrictions and guidelines:

- Before the upgrade, make sure each IRF member's flash memory has free space that is at least twice the image file size.
- During the upgrade, make sure the following requirements are met:
  - Do not execute any commands that are not for the ISSU.
  - Prevent other operators from operating the device.

Upgrade procedures

Download the image file from the TFTP server to the root directory of the master's flash memory.

```
<Sysname> tftp 2.2.2.2 get example.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                 Dload  Upload   Total   Spent    Left  Speed
100 42.8M  100 42.8M    0     0   159k      0  0:04:34  0:04:34 --:--:--  165k
```

Display the current active software images on the IRF members.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 2:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
Active packages on slot 3:
  flash:/boot-r2210.bin
  flash:/system-r2210.bin
```

Identify the recommended ISSU method and its possible impacts on the device.

```
<Sysname> display version comp-matrix file ipe flash:/example.ipe
Boot image: boot-r2211.bin
  Version:
  7.1.035P02

System image: system-r2211.bin
  Version:
  R2211
  Version compatibility list:
  R2211
  Version dependency boot list:
  7.1.035P02
Incompatible upgrade.
```

The output shows the following information:

- The two versions are incompatible.
- The incompatible upgrade method is recommended.
- The IRF members will be rebooted during the upgrade.

Upgrade IRF member 3.

```
<Sysname> issu load file ipe flash:/example.ipe slot 3
This operation will delete the rollback point information for the previous upgrade
```

```
and maybe get unsaved configuration lost. Continue? [Y/N]:y
Successfully copied flash:/boot-r2211.bin to slot3#flash:/boot-r2211.bin.
Successfully copied flash:/system-r2211.bin to slot2#flash:/system-r2211.bin.

flash:/boot-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

flash:/system-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

  Slot  Upgrade Way
  3     Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]: y
```

IRF member 3 reboots to load the new images.

Verify that IRF member 3 has loaded the new images.

```
<Sysname> display issu state
 ISSU state: Loaded
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: slot 3
Current upgrading slot: None
Current version list:
  boot: 7.1.035P02
  system: Comware V700R001B35D603
Current software images:
  flash:/s5900_5920-cmw710-boot-r2211.bin
  flash:/s5900_5920-cmw710-system-r2211.bin
```

After IRF member 3 loads the new images, the **ISSU state** field displays **Loaded**.

NOTE:

After you upgrade an IRF member, make sure the upgrade has been completed on the member before you continue with the following steps.

Perform a master/subordinate switchover to upgrade IRF member 1 and IRF member 2.

```
<Sysname> issu run switchover
Successfully copied flash:/boot-r2211.bin to slot2#flash:/boot-r2211.bin.
Successfully copied flash:/system-r2211.bin to slot2#flash:/system-r2211.bin.

flash:/boot-r2211.bin
  Running Version             New Version
  Release 2210                Release 2211

flash:/system-r2211.bin
  Running Version             New Version
```

```
  Release 2210                Release 2211

  Slot  Upgrade Way
  2     Reboot
  1     Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
```

IRF member 1 and IRF member 2 reboot to load the new images.

Verify that the two IRF members has loaded the new images.

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
Current version list:
  boot: 7.1.035P02
  system: Comware V700R001B35D603
Current software images:
  flash:/s5900_5920-cmw710-boot-r2211.bin
  flash:/s5900_5920-cmw710-system-r2211.bin
```

After the two IRF members load the new images, the **ISSU state** field displays **Init**, and the entire ISSU process is completed.

Verifying the upgrade

Verify that the IRF members are running the new images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r2211.bin
  flash:/system-r2211.bin
Active packages on slot 2:
  flash:/boot-r2211.bin
  flash:/system-r2211.bin
Active packages on slot 3:
  flash:/boot-r2211.bin
  flash:/system-r2211.bin
```

Configuration files

The system does not save the commands used in the procedures to a configuration file.

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 5920	Release 2208P01
HP 5900	Release 2210

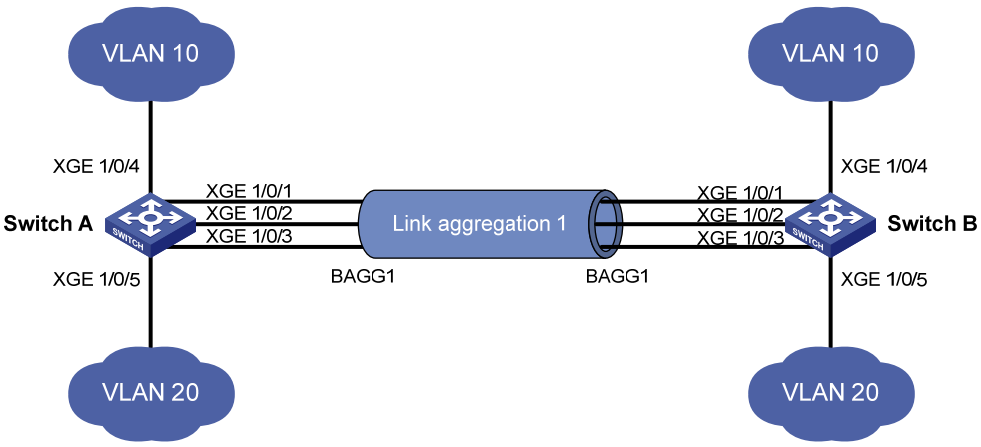
Network requirements

As shown in Figure 114, 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:

- VLAN 10 on Switch A can communicate with VLAN 10 on Switch B. VLAN 20 on Switch A can communicate with VLAN 20 on Switch B.
- The packets between Switch A and Switch B are load-shared across the Selected ports of the link aggregation group by source MAC address and destination MAC address.

Figure 114 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To enable traffic from VLAN 10 and VLAN 20 to pass through Layer 2 aggregate interface 1, perform the following tasks:
  - Configure Layer 2 aggregate interface 1 as a trunk port.

- Assign the aggregate interface to VLAN 10 and VLAN 20.

- To load-share packets between Switch A and Switch B across the Selected ports of the link aggregation group, configure the load sharing criteria in either of the following views:
  - System view.
  - Aggregate interface view.

  This example uses the system view.

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 interface view to check the following attribute configurations of the port:
     - Port isolation configuration.
     - QinQ configuration.
     - VLAN configuration.
  b. If any of the above configurations exist, use the **undo** forms of the corresponding commands to remove these configurations. This enables the port to use the default attribute configurations.
  c. Assign the port to an aggregation group.
- In a static aggregation group, the Selected state of a port is not affected by whether the peer port is added to an aggregation group and is Selected. As a result, the Selected state of a port might be different from the Selected state of the peer port. When both ends support static aggregation and dynamic aggregation, HP recommends that you preferentially use dynamic aggregation.
- You cannot assign a port to a Layer 2 aggregation group when MAC authentication, port security mode, or 802.1X is configured or enabled on the port.

Configuration procedures

Configuring Switch A

Enter system view, and configure the link aggregation load sharing criteria as source MAC address and destination MAC address.

```
<SwitchA> system-view
[SwitchA] link-aggregation global load-sharing mode source-mac destination-mac
```

Create VLAN 10, and assign port Ten-GigabitEthernet 1/0/4 to VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port ten-gigabitethernet 1/0/4
[SwitchA-vlan10] quit
```

Create VLAN 20, and assign port Ten-GigabitEthernet 1/0/5 to VLAN 20.

```
[SwitchA] vlan 20
[SwitchA-vlan20] port ten-gigabitethernet 1/0/5
[SwitchA-vlan20] quit
```

Create Layer 2 aggregate interface 1. (Choose one of the following methods as needed.)

- Use the static aggregation mode to create Layer 2 aggregate interface 1.

```
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] quit
```

- Use the dynamic aggregation mode to create Layer 2 aggregate interface 1.

```
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation1] quit
```

Assign ports Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to aggregation group 1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-Ten-GigabitEthernet1/0/2] quit
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-Ten-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
 Configuring Ten-GigabitEthernet1/0/1 done.
 Configuring Ten-GigabitEthernet1/0/2 done.
 Configuring Ten-GigabitEthernet1/0/3 done.
[SwitchA-Bridge-Aggregation1] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Use the **display link-aggregation verbose** command to display detailed information about the link aggregation groups to verify whether the configuration is successful.

- Link aggregation configuration 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
--------------------------------------------------------------------------------
  XGE1/0/1          S       32768     1
```

```
  XGE1/0/2          S       32768     1
  XGE1/0/3          S       32768     1
```

The output shows that all member ports in the local aggregation group are in Selected state. The Selected states of the local member ports are not affected by the Selected states of the peer member ports.

- Link aggregation configuration 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: Bridge-Aggregation11
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e234-5678
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  XGE1/0/1          S       32768    1         {ACDEF}
  XGE1/0/2          S       32768    1         {ACDEF}
  XGE1/0/3          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  XGE1/0/1          14      32768    1         0x8000, 0000-fc00-7506 {ACDEF}
  XGE1/0/2          15      32768    1         0x8000, 0000-fc00-7506 {ACDEF}
  XGE1/0/3          16      32768    1         0x8000, 0000-fc00-7506 {ACDEF}
```

The output shows that the local member ports and the corresponding peer member ports are all Selected. In the dynamic link aggregation mode, each local member port and the corresponding peer member port have the same Selected state through exchanging LACPDUs. The user data traffic can be correctly forwarded.

Configuration files

- Switch A:

```
#
link-aggregation global load-sharing mode source-mac destination-mac
#
vlan 10
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 10
#
vlan 20
#
interface Ten-GigabitEthernet1/0/5
```

```
 port access vlan 20
```

- In the static aggregation mode:

```
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 10 20
```

- In the dynamic aggregation mode:

```
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 10 20
link-aggregation mode dynamic
```

```
#
interface Ten-GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
```

- Switch B:

  The configuration file on Switch B is the same as the configuration file on Switch A.

Example: Configuring Layer 2 link aggregation load sharing

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

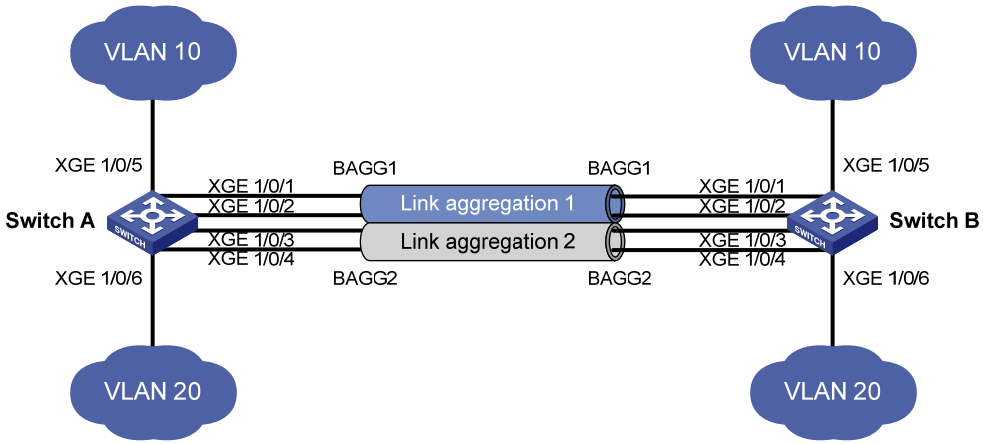
Network requirements

As shown in Figure 115, 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:

- VLAN 10 on Switch A can communicate with VLAN 10 on Switch B. VLAN 20 on Switch A can communicate with VLAN 20 on Switch B.
- The packets from VLAN 10 are load-shared across the Selected ports of a link aggregation group by source MAC address. The packets from VLAN 20 are load-shared across the Selected ports of a link aggregation group by destination MAC address.

Figure 115 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To configure different load sharing criteria for packets in different link aggregation groups, configure link aggregation load sharing criteria in Layer 2 aggregate interface view.
- To enable packets from VLAN 10 to pass through aggregate interface 1, assign aggregate interface 1 to VLAN 10. To enable packets from VLAN 20 to pass through aggregate interface 2, 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 interface view to check the following attribute configurations of the port:
     - Port isolation configuration.
     - QinQ configuration.
     - VLAN configuration.
  b. If any of the above configurations exist, use the **undo** forms of the corresponding commands to remove these configurations. This enables the port to use the default attribute configurations.
  c. Assign the port to an aggregation group.
- You cannot assign a port to a Layer 2 aggregation group when MAC authentication, port security mode, or 802.1X is configured or enabled on the port.

Configuration procedures

Configuring Switch A

Create VLAN 10, and assign port Ten-GigabitEthernet 1/0/5 to VLAN 10.

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] port ten-gigabitethernet 1/0/5
[SwitchA-vlan10] quit
```

Create VLAN 20, and assign port Ten-GigabitEthernet 1/0/6 to VLAN 20.

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-vlan20] port ten-gigabitethernet 1/0/6
[SwitchA-vlan20] quit
```

Create Layer 2 aggregate interface 1.

```
[SwitchA] interface bridge-aggregation 1
```

Configure the link aggregation load sharing criterion 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 1.

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

Assign Layer 2 aggregate interface 1 to VLAN 10.

```
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] port access vlan 10
Configuring Ten-GigabitEthernet1/0/1 done.
Configuring Ten-GigabitEthernet1/0/2 done.
[SwitchA-Bridge-Aggregation1] quit
```

Create Layer 2 aggregate interface 2.

```
[SwitchA] interface bridge-aggregation 2
```

Configure the link aggregation load sharing criterion 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 Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 2.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-aggregation group 2
[SwitchA-Ten-GigabitEthernet1/0/3] quit
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] port link-aggregation group 2
[SwitchA-Ten-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
Configuring Ten-GigabitEthernet1/0/3 done.
Configuring Ten-GigabitEthernet1/0/4 done.
[SwitchA-Bridge-Aggregation2] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Display the information about Selected ports in link aggregation groups.

```
[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
--------------------------------------------------------------------------------
  XGE1/0/1         S       32768     1
  XGE1/0/2         S       32768     1

Aggregation Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority  Oper-Key
--------------------------------------------------------------------------------
  XGE1/0/3         S       32768     2
  XGE1/0/4         S       32768     2
```

The output shows that:

- 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.

Display the link aggregation load sharing criteria.

```
[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 that:

- The link aggregation load sharing criteria for Layer 2 aggregate interface 1 is source MAC address.
- The link aggregation load sharing criteria for Layer 2 aggregate interface 2 is destination MAC address.

Configuration files

- Switch A:

```
#
vlan 10
#
interface Ten-GigabitEthernet1/0/5
port access vlan 10
#
vlan 20
#
interface Ten-GigabitEthernet1/0/6
port access vlan 10
#
interface Bridge-Aggregation1
port access vlan 10
link-aggregation load-sharing mode source-mac
#
interface Ten-GigabitEthernet1/0/1
port access vlan 10
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
port access vlan 10
port link-aggregation group 1
#
interface Bridge-Aggregation2
port access vlan 20
link-aggregation load-sharing mode destination-mac
#
interface Ten-GigabitEthernet1/0/3
port access vlan 20
port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/4
port access vlan 20
port link-aggregation group 2
```

- Switch B:

  The configuration file on Switch B is the same as the configuration file on Switch A.

LLDP configuration examples

This chapter provides LLDP configuration examples.

Example: Configuring basic LLDP

Applicable product matrix

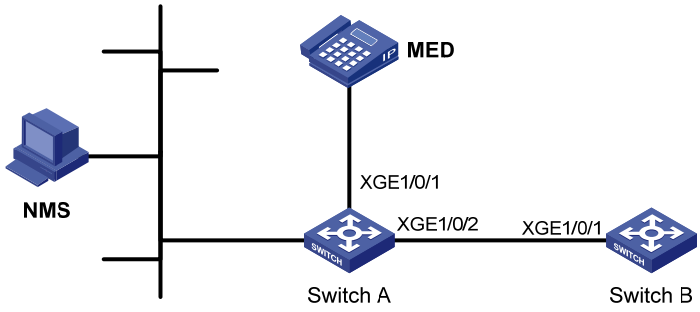
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 116, 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 116 Network diagram



Configuration restrictions and guidelines

To view log information about neighbor changes on the terminal screen, make sure the following features are enabled:

- Monitoring system information on the current terminal. By default, this feature is disabled. Use the **terminal monitor** command in user view to enable the monitor feature.
- Displaying log information on the current terminal. By default, this feature is enabled. Use the **terminal logging** command in user view to enable the display feature.
- Information center. By default, this feature is enabled. Use the **info-center enable** command in system view to enable the information center feature.

For more information, see *Network Management and Monitoring Configuration Guide* in *HP 5920 & 5900 Switch Series Configuration Guides*.

Configuration procedures

1. Configure Switch A:

   # Enable LLDP globally.

   By default:

   - When the switch starts with zero configurations, LLDP is globally disabled.
   - When the device starts with default configurations, LLDP is globally enabled.

   ```
   <SwitchA> system-view
   [SwitchA] lldp global enable
   ```

   # Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
   ```

   # Set the LLDP operating mode to Rx.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp admin-status rx
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Enable LLDP on Ten-GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] lldp enable
   ```

   # Set the LLDP operating mode to Rx.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/2] lldp admin-status rx
   [SwitchA-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure Switch B:

   # Enable LLDP globally.

   By default:

   - When the switch starts with zero configurations, LLDP is globally disabled.
   - When the device starts with default configurations, LLDP is globally enabled.

   ```
   <SwitchB> system-view
   [SwitchB] lldp global enable
   ```

   # Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

   ```
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] lldp enable
   ```

   # Set the LLDP operating mode to Rx.

   ```
   [SwitchB-Ten-GigabitEthernet1/0/1] lldp admin-status tx
   [SwitchB-Ten-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

LLDP status information of Port 1 [Ten-GigabitEthernet1/0/1]:
Port status of LLDP              : Enable
Admin status                     : Rx_Only
Trap flag                        : No
MED trap flag                    : No
Polling interval                 : 0s
Number of LLDP neighbors         : 1
Number of MED neighbors          : 1
Number of CDP neighbors          : 0
Number of sent optional TLV      : 21
Number of received unknown TLV   : 0

LLDP status information of Port 2 [Ten-GigabitEthernet1/0/2]:
Port status of LLDP              : Enable
Admin status                     : Rx_Only
Trap flag                        : No
MED trap flag                    : No
Polling interval                 : 0s
Number of LLDP neighbors         : 1
Number of MED neighbors          : 0
Number of CDP neighbors          : 0
Number of sent optional TLV      : 21
Number of received unknown TLV   : 0
```

The output shows that:

- Ten-GigabitEthernet 1/0/1 of Switch A connects to an MED device.
- Ten-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 then 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
```

```
LLDP status information of Port 1 [Ten-GigabitEthernet1/0/1]:
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 1
Number of MED neighbors         : 1
Number of CDP neighbors         : 0
Number of sent optional TLV     : 21
Number of received unknown TLV  : 0

LLDP status information of Port 2 [Ten-GigabitEthernet1/0/2]:
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 21
Number of received unknown TLV  : 0
```

The output shows that Ten-GigabitEthernet 1/0/2 of Switch A is not connected to any neighboring devices.

Configuration files

- Switch A:

```
#
 lldp global enable
#
interface Ten-GigabitEthernet1/0/1
 lldp admin-status rx
#
interface Ten-GigabitEthernet1/0/2
 lldp admin-status rx
#
```

- Switch B:

```
#
 lldp global enable
#
interface Ten-GigabitEthernet1/0/1
 lldp admin-status tx
#
```

Login management configuration examples

This document provides examples for configuring the following:

- Console login.
- Telnet login.
- Login authentication.
- Command authorization.
- Command accounting.

Example: Configuring console login

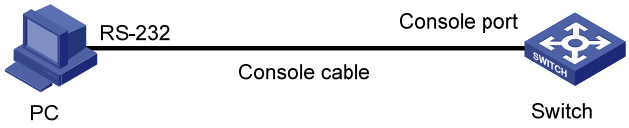
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 117, use the console port of the switch for the first login. After login, configure local authentication so a console user must provide the correct username and password to log in to the switch.

Figure 117 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To log in to the switch, you are only required to make sure the terminal is using the same communication settings as the console port. By default, console login is enabled and authentication is not required.

  The default settings for the console port are as follows:

  - **Bits per second**—9600 bps
  - **Flow control**—None
  - **Parity**—None
  - **Stop bits**—1
  - **Data bits**—8

- To configure local authentication for console users, you must set the authentication mode to scheme for the AUX user interface and configure a local user.
- To enable a local user to log in through the console port and manage the switch, you must assign the terminal service and the user role network-admin to the user. By default, a local user cannot use any service and is assigned the user role network-operator.

Configuration procedures

On the PC, run a terminal emulation program and create a connection, as shown in Figure 118 and Figure 119.

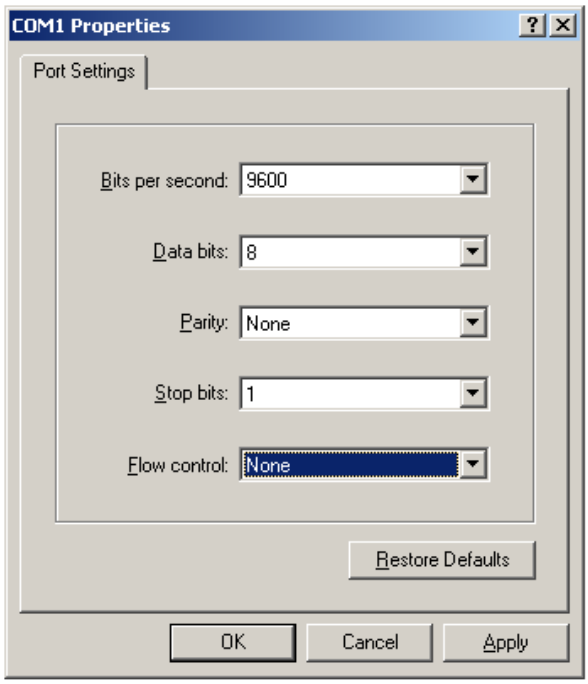
In this example, the PC is running Windows XP. On Windows Server 2003, you must add the HyperTerminal program first. On Windows Server 2008, Windows 7, Windows Vista, or other operating systems, you must obtain a third-party terminal control program first. Follow the user guide or online help for the program to log in to the switch.

Figure 118 Creating a connection

Figure 119 Specifying the connection port

Set communication parameters, as shown in Figure 120.

Figure 120 Setting communication parameters



Power on the switch.

After the switch starts up, the prompt <HP> appears.

Enter user interface AUX 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
```

Set the authentication mode to **scheme**.

```
[Sysname-ui-aux0] authentication-mode scheme
```

Exit to system view.

```
[Sysname-ui-aux0] quit
```

Create local user **admin**.

```
[Sysname] local-user guest
New local user added.
```

Set the password to **123**.

```
[Sysname-luser-manage-guest] password simple 123
```

Assign the terminal service and the user role network-admin to the user.

```
[Sysname-luser-manage-guest] service-type terminal
[Sysname-luser-manage-guest] authorization-attribute user-role network-admin
[Sysname-luser-manage-guest] quit
```

Verifying the configuration

Terminate the current connection. (Details not shown.)

Log in to the switch through the console port again. Verify that you must provide the configured username and password to log in. (Details not shown.)

Configuration files

```
#
local-user guest class manage
 password hash
$h$6$R1DZqFZrkA93GMAf$th9k1FcsjqRRy1A2reQXQkfmnTBSr/7//80W5gKuyeHYxNor/FVNl4tbBQLhaGe
Y5XFrVr1+WopPcC+dfaumgg==
 service-type terminal
 authorization-attribute user-role network-admin
#
user-interface aux 0
 authentication-mode scheme
```

Example: Configuring Telnet login

Applicable product matrix

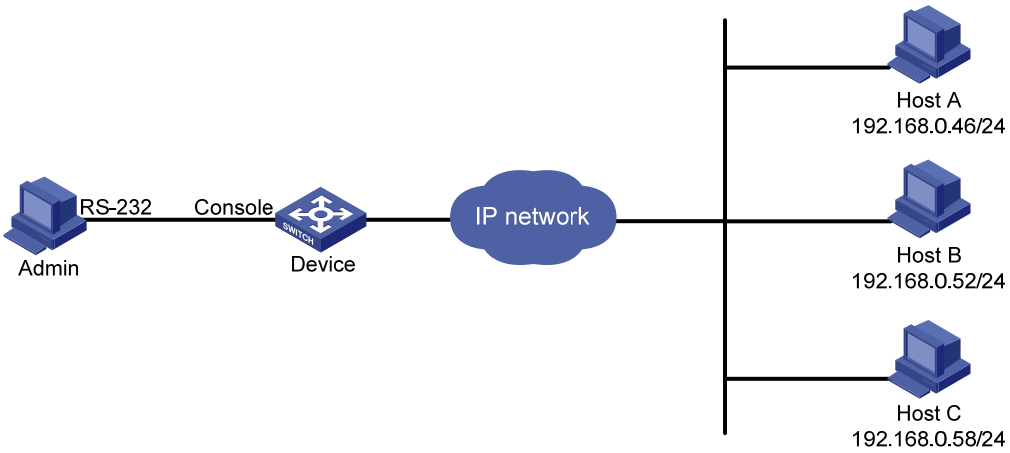
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 121, configure the switch to achieve the following goals:

- Host A and Host B can Telnet to the switch without authentication and manage the switch.
- Other hosts cannot Telnet to the switch.

Figure 121 Network diagram



Requirements analysis

By default, Telnet login is disabled. To enable Telnet login, you must enable the Telnet server function.

The default user role is network-operator for a Telnet user. To enable Telnet users to manage the switch, you must assign the user role network-admin to the VTY user interfaces.

Configuration procedures

Enable the Telnet server function.

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

Disable authentication for Telnet users.

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode none
```

Assign the user role network-admin to Telnet users.

```
[Sysname-ui-vty0-15] user-role network-admin
[Sysname-ui-vty0-15] quit
```

Create basic ACL 2000.

```
[Sysname] acl number 2000
```

Define a rule to permits only packets from 192.168.0.52 and 192.168.0.46.

```
[Sysname-acl-basic-2000] rule 1 permit source 192.168.0.52 0
[Sysname-acl-basic-2000] rule 2 permit source 192.168.0.46 0
[Sysname-acl-basic-2000] rule 3 deny source any
[Sysname-acl-basic-2000] quit
```

Use the ACL to control Telnet user access.

```
[Sysname] telnet server acl 2000
```

Verifying the configuration

Verify that Host A and Host B can Telnet to the switch. (Details not shown.)

Verify that Host C cannot Telnet to the switch. (Details not shown.)

Configuration files

```
#
 telnet server enable
 telnet server acl 2000
#
acl number 2000
 rule 1 permit source 192.168.0.52 0
 rule 2 permit source 192.168.0.46 0
 rule 3 deny
#
user-interface vty 0 15
```

```
 authentication-mode none
 user-role network-admin
#
```

Example: Configuring login authentication and command authorization

Applicable product matrix

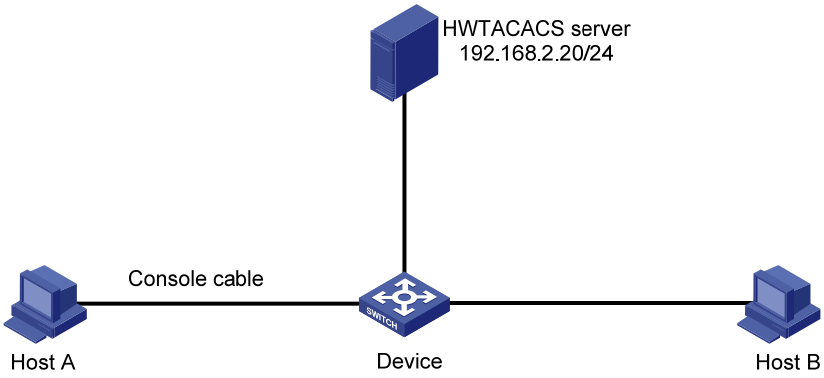
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 122, configure the switch to achieve the following goals:

- Console and Telnet users must provide the correct username and password to log in to the switch.
- The switch uses the HWTACACS server for login user authentication. If the HWTACACS server is not available, the switch performs local authentication.
- The switch uses the HWTACACS server for command authorization. If the HWTACACS server is not available, the switch performs local command authorization.

Figure 122 Network diagram



Requirements analysis

For console and VTY users to provide a username and password at login, you must enable scheme authentication on the AUX and VTY user interfaces.

For command authorization, you must configure command authorization on the AUX and VTY user interfaces.

To use the HWTACACS server for user authentication and command authorization and use local authentication and authorization for backup, you must do the following:

- Configure an HWTACACS scheme on the switch.
- Configure local user accounts on the switch.
- Configure the switch to use the HWTACACS scheme for login user authentication and authorization and use local authentication and authorization for backup.

Configuration restrictions and guidelines

Complete the required configurations on the HWTACACS server before enabling command authorization on the switch. The command authorization function takes effect immediately to control user access to commands.

Configuration procedures

1. Assign IP addresses to interfaces so the switch can communicate with the HWTACACS server, Host A, and Host B. (Details not shown.)
2. Configure the HWTACACS scheme **tac**:

   # Create HWTACACS scheme **tac**.

   ```
   <Device> system-view
   [Device] hwtacacs scheme tac
   ```

   # Use the HWTACACS server at 192.168.2.20:1812 for authentication.

   ```
   [Device-hwtacacs-tac] primary authentication 192.168.2.20 1812
   ```

   # Use the shared key **expert** for authentication communication.

   ```
   [Device-hwtacacs-tac] key authentication simple expert
   ```

   # Use the HWTACACS server at 192.168.2.20:49 for authorization.

   ```
   [Device-hwtacacs-tac] primary authorization 192.168.2.20 49
   ```

   # Use the shared key **expert** for authorization communication.

   ```
   [Device-hwtacacs-tac] key authorization simple expert
   ```

   # Remove domain names from usernames sent to the HWTACACS server.

   ```
   [Device-hwtacacs-tac] user-name-format without-domain
   [Device-hwtacacs-tac] quit
   ```

3. Configure the system-predefined domain **system**:

   # Use HWTACACS scheme **tac** for login user authentication. Use local authentication as the backup method.

   ```
   [Device] domain system
   [Device-isp-system] authentication login hwtacacs-scheme tac local
   ```

   # Use HWTACACS scheme **tac** for login user command authorization. Use local authorization as the backup method.

   ```
   [Device-isp-system] authorization command hwtacacs-scheme tac local
   [Device-isp-system] quit
   ```

4. Configure local user **adminc** for the console user:

   # Create local user **adminc**.

   ```
   [Device] local-user adminc
   ```

   # Set the password to **adminc**.

   ```
   [Device-luser-manage-adminc] password simple adminc
   ```

Assign the terminal service and the network-admin user role to the user.

```
[Device-luser-manage-adminc] service-type terminal
[Device-luser-manage-adminc] authorization-attribute user-role network-admin
[Device-luser-manage-adminc] quit
```

5. Configure local user **admint** for the Telnet user:

   # Create local user **admint**.

   ```
   [Device] local-user admint
   ```

   # Set the password to **admint**.

   ```
   [Device-luser-manage-admint] password simple admint
   ```

   # Assign the Telnet service and the network-admin user role to the user.

   ```
   [Device-luser-manage-admint] service-type telnet
   [Device-luser-manage-admint] authorization-attribute user-role network-admin
   [Device-luser-manage-admint] quit
   ```

6. Enable the Telnet server function.

   ```
   [Device] telnet server enable
   ```

7. Enable scheme authentication and command authorization for user interface AUX 0.

   ```
   [Device] user-interface aux 0
   [Device-ui-aux0] authentication-mode scheme
   [Device-ui-aux0] command authorization
   [Device-ui-aux0] quit
   ```

8. Enable scheme authentication and command authorization for user interfaces VTY 0 through VTY 15.

   ```
   [Device] user-interface vty 0 15
   [Device-ui-vty0-15] authentication-mode scheme
   [Device-ui-vty0-15] command authorization
   [Device-ui-vty0-15] quit
   ```

Verifying the configuration

1. Verify that the console and Telnet users must provide the correct username and password to log in to the switch. (Details not shown.)
2. Verify that the console and Telnet users can perform only authorized commands. (Details not shown.)
3. Verify that the switch uses the HWTACACS server for login user authentication. If the HWTACACS server is not available, the switch performs local authentication. (Details not shown.)
4. Verify that the switch uses the HWTACACS server for command authorization. If the HWTACACS server is not available, the switch performs local command authorization. (Details not shown.)

Configuration files

```
#
 telnet server enable
#
user-interface aux 0
 authentication-mode scheme
 command authorization
```

```
#
user-interface vty 0 15
 authentication-mode scheme
 command authorization
#
hwtacacs scheme tac
 primary authentication 192.168.2.20 1812
 primary authorization 192.168.2.20
 key authentication cipher $c$3$FXiz27yo30K7lGsWqrc6skZDpX8+PIBLNQ==
 key authorization cipher $c$3$Nv66yberLu35cO+Faby9wY9LwmUHJXeekg==
 user-name-format without-domain
#
domain system
 authentication login hwtacacs-scheme tac local
 authorization command hwtacacs-scheme tac local
#
local-user adminc class manage
 password hash
$h$6$wbU0m+ZTRgUENvWl$arSsauK2X85OVbJo+TzLOl0AcH3klbKRWLXDdlVEAEUucfCFAXjHDKFdhsclBci
0bW3+M8zsEuWIaYV6Xarw1g==
 service-type terminal
 authorization-attribute user-role network-admin
#
local-user admint class manage
 password hash
$h$6$9mVCOb4kH1bbnTMG$5Z5gO245ak/GiYnrnqEQc/G9YyG1MOOcfA/g20CGWjUMdhAGIJ134dN2G7Lerhq
iIofo3F0HwlvxFUHSTvrs9A==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

Example: Configuring login authentication and command accounting

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

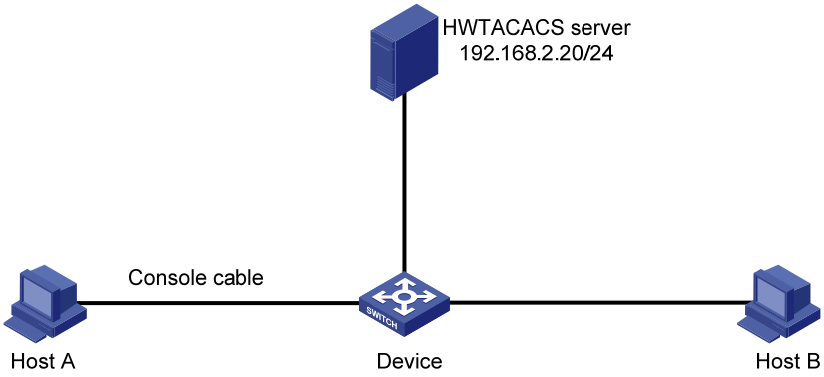
Network requirements

As shown in Figure 123, configure the switch to achieve the following goals:

- Console and Telnet users must provide the correct username and password to log in to the switch.

- The switch uses the HWTACACS server for login user authentication. If the HWTACACS server is not available, the switch performs local authentication.
- The switch uses the HWTACACS server for command accounting.

Figure 123 Network diagram



Requirements analysis

For console and VTY users to provide a username and password at login, you must enable scheme authentication on the AUX and VTY user interfaces.

For command accounting, you must configure command accounting on the AUX and VTY user interfaces.

To use the HWTACACS server for user authentication and command accounting and use local authentication for backup, you must do the following:

- Configure an HWTACACS scheme on the switch.
- Configure local user accounts on the switch.
- Configure the switch to use the HWTACACS scheme for login user authentication and accounting and to use local authentication for backup.

Configuration procedures

1. Assign IP addresses to interfaces so the switch can communicate with the HWTACACS server, Host A, and Host B. (Details not shown.)
2. Configure HWTACACS scheme **tac**:

   # Create HWTACACS scheme **tac**.

   ```
   <Device> system-view
   [Device] hwtacacs scheme tac
   ```

   # Use the HWTACACS server at 192.168.2.20:1812 for authentication.

   ```
   [Device-hwtacacs-tac] primary authentication 192.168.2.20 1812
   ```

   # Use the shared key **expert** for authentication communication.

   ```
   [Device-hwtacacs-tac] key authentication simple expert
   ```

   # Use the HWTACACS server at 192.168.2.20:49 for accounting.

   ```
   [Device-hwtacacs-tac] primary accounting 192.168.2.20 49
   ```

   # Use the shared key **expert** for accounting communication.

```
[Device-hwtacacs-tac] key accounting simple expert
```

Remove domain names from usernames sent to the HWTACACS server.

```
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```

3. Configure the system-predefined domain **system**:

Use HWTACACS scheme **tac** for login user authentication. Use local authentication as the backup method.

```
[Device] domain system
[Device-isp-system] authentication login hwtacacs-scheme tac local
```

Use HWTACACS scheme **tac** for login user command accounting.

```
[Device-isp-system] accounting command hwtacacs-scheme tac
[Device-isp-system] quit
```

4. Configure local user **adminc** for the console user:

Create local user **adminc**.

```
[Device] local-user adminc
```

Set the password to **adminc**.

```
[Device-luser-manage-adminc] password simple adminc
```

Assign the terminal service and the network-admin user role to the user.

```
[Device-luser-manage-adminc] service-type terminal
[Device-luser-manage-adminc] authorization-attribute user-role network-admin
[Device-luser-manage-adminc] quit
```

5. Configure local user **admint** for the Telnet user:

Create local user **admint**.

```
[Device] local-user admint
```

Set the password to **admint**.

```
[Device-luser-manage-admint] password simple admint
```

Assign the Telnet service and the network-admin user role to the user.

```
[Device-luser-manage-admint] service-type telnet
[Device-luser-manage-admint] authorization-attribute user-role network-admin
[Device-luser-manage-admint] quit
```

6. Enable the Telnet server function.

```
[Device] telnet server enable
```

7. Enable scheme authentication and command accounting for user interface AUX 0.

```
[Device] user-interface aux 0
[Device-ui-aux0] authentication-mode scheme
[Device-ui-aux0] command accounting
[Device-ui-aux0] quit
```

8. Enable scheme authentication and command accounting for user interfaces VTY 0 through VTY 15.

```
[Device] user-interface vty 0 15
[Device-ui-vty0-15] authentication-mode scheme
[Device-ui-vty0-15] command accounting
[Device-ui-vty0-15] quit
```

Verifying the configuration

1. Verify that the console and Telnet users must provide the correct username and password to log in to the switch. (Details not shown.)
2. Verify that the switch uses the HWTACACS server for login user authentication. If the HWTACACS server is not available, the switch performs local authentication. (Details not shown.)
3. Verify that the switch uses the HWTACACS server for command accounting. If the HWTACACS server is not available, the switch performs local command accounting. (Details not shown.)

Configuration files

```
#
 telnet server enable
#
hwtacacs scheme tac
 primary authentication 192.168.2.20 1812
 primary accounting 192.168.2.20
 key authentication cipher $c$3$2CoitG8Bv/pXpRVVeXZqVcOEwOYIStxviw==
 key accounting cipher $c$3$3J4gt4wqCQoAVEFSqGIbW5kQW+C0kKN0kg==
 user-name-format without-domain
#
domain system
 authentication login hwtacacs-scheme tac local
 accounting command hwtacacs-scheme tac
#
local-user adminc class manage
 password hash
$h$6$8ImBlxRLI6rEAXsY$WOi2HrT5xYRRN8ylN74lqEk/ee3JzqtLW7xYlX8LqxTVdyBROk2wD2IS3FPsL8N
W06brD/wtsrOGA79BjZIlnQ==
 service-type terminal
 authorization-attribute user-role network-admin
#
local-user admint class manage
 password hash
$h$6$fDujw2DCcq4gD1zu$gDQHvxjeeq4cRT4bwDEDxVnuPunQHiJvLRuAPtgE8EsRKK9BBAqdDyT+AfPEJXm
V7wzgry6x3YaF3T4PmHq7Ig==
 service-type telnet
 authorization-attribute user-role network-admin
#
user-interface aux 0
 authentication-mode scheme
 command accounting
user-interface vty 0 15
 authentication-mode scheme
 command accounting
#
```

Loop detection configuration examples

This chapter provides examples for detecting Layer 2 loops by using the loop detection loop function.

General configuration restrictions and guidelines

HP recommends not enabling loop detection on TRILL ports, because TRILL networks prevent loops from being generated. For information more about TRILL, see *TRILL Configuration Guide*.

Example: Configuring loop detection

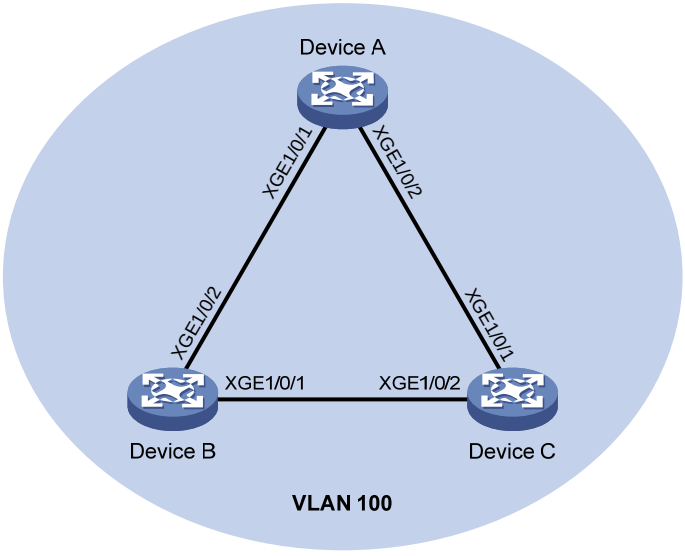
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 124, configure loop detection on Device A, so that Device A generates a log as a notification and automatically shuts down the port on which a loop is detected.

Figure 124 Network diagram



Configuration procedures

1. Configure Device A:

Create VLAN 100, and globally enable loop detection for the VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

Configure Ten-GigabitEthernet1/0/1 and Ten-GigabitEthernet1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

Configure the global loop protection action as shutdown.

```
[DeviceA] loopback-detection global action shutdown
```

Set the loop detection interval to 35 seconds.

```
[DeviceA] loopback-detection interval-time 35
```

2. Configure Device B:

Create VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB–vlan100] quit
```

Configure Ten-GigabitEthernet1/0/1 and Ten-GigabitEthernet1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-Ten-GigabitEthernet1/0/1] quit
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

3. Configure Device C:

Create VLAN 100.

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC–vlan100] quit
```

Configure Ten-GigabitEthernet1/0/1 and Ten-GigabitEthernet1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceC] interface ten-gigabitethernet 1/0/1
[DeviceC-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-Ten-GigabitEthernet1/0/1] quit
[DeviceC] interface ten-gigabitethernet 1/0/2
[DeviceC-Ten-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceC-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

After the configurations are complete, Device A detects loops on ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 within a loop detection interval. Consequently, Device A automatically shuts down the ports and generates the following log messages:

```
[DeviceA]
%Feb 24 15:04:29:663 2013 DeviceA LPDT/4/LPDT_LOOPED: Loopback exists on
Ten-GigabitEthernet1/0/1.
%Feb 24 15:04:29:667 2013 DeviceA LPDT/4/LPDT_LOOPED: Loopback exists on
Ten-GigabitEthernet1/0/2.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT_RECOVERED: Loopback on
Ten-GigabitEthernet1/0/1 recovered.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT_RECOVERED: Loopback on
Ten-GigabitEthernet1/0/2 recovered.
```

Display the loop detection configuration and status on Device A.

```
[DeviceA] display loopback-detection
Loop detection is enabled.
Loop detection interval is 35 second(s).
No loopback is detected.
```

The output shows that the device has removed the loops from Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 according to the shutdown action.

Display the status of Ten-GigabitEthernet 1/0/1 on Device A.

```
[DeviceA] display interface ten-gigabitethernet 1/0/1
 Ten-GigabitEthernet1/0/1 current state: DOWN (Loopback detection down)
...
```

Display the status of Ten-GigabitEthernet 1/0/2 on Device A.

```
[DeviceA] display interface ten-gigabitethernet 1/0/2
 Ten-GigabitEthernet1/0/2 current state: DOWN (Loopback detection down)
...
```

The output shows that Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are already shut down by the loop detection module.

To open the ports that are shut down, use the **undo shutdown** command. (Details not shown.)

Configuration files

- Device A

```
#
vlan 100
#
 loopback-detection global enable vlan 100
 loopback-detection global action shutdown
 loopback-detection interval-time 35
```

```
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- Device B

```
#
vlan 100
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- Device C

  The configuration files on device C is the same as that on device B.

MAC address table configuration examples

This chapter provides typical application scenarios and configuration examples for the following MAC address entries:

- Static MAC address entries.
- Dynamic MAC address entries.
- Blackhole MAC address entries.

Example: Configuring the MAC address table

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

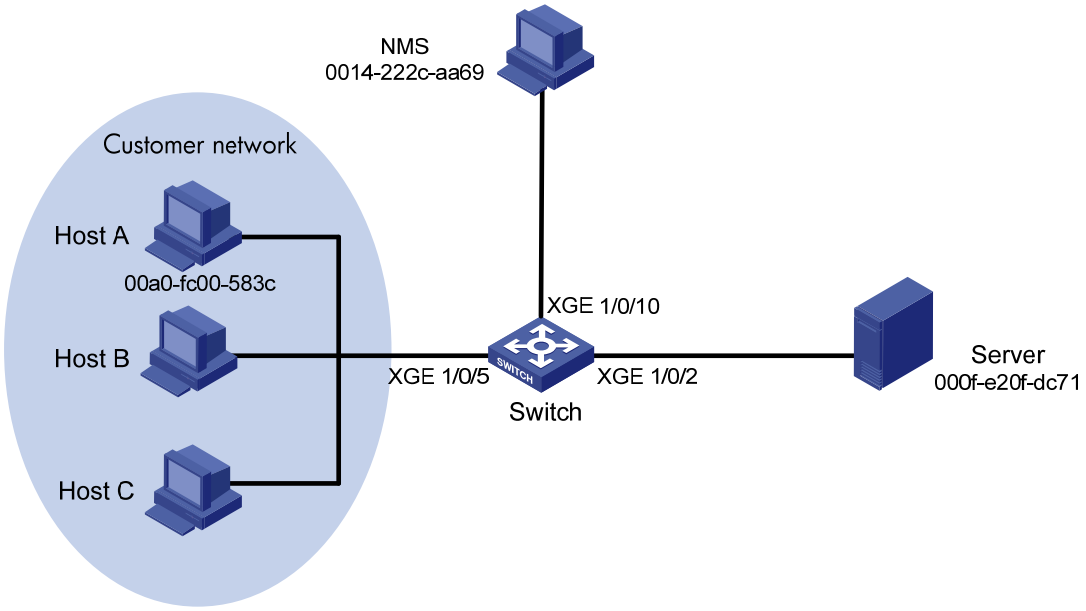
Network requirements

As shown in Figure 125, 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 through interface Ten-GigabitEthernet 1/0/2.
- The switch uses a static MAC address entry to forward frames destined for the NMS through interface Ten-GigabitEthernet 1/0/10.
- Interface Ten-GigabitEthernet 1/0/10 provides access for only the NMS.
- Interface Ten-GigabitEthernet 1/0/5 that connects to the customer network generates MAC address entries through learning source MAC addresses of incoming frames.
- The switch does not forward frames sourced from the host that launches attacks (Host A in this example).

Figure 125 Network diagram



Requirements analysis

To meet the network requirements, perform the following tasks:

- To allow interface Ten-GigabitEthernet 1/0/10 to provide access for only the NMS, set the MAC address learning limit to 0 on Ten-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 Ten-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 Ten-GigabitEthernet 1/0/2, Ten-GigabitEthernet 1/0/5, and Ten-GigabitEthernet 1/0/10 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port Ten-GigabitEthernet1/0/2 Ten-GigabitEthernet1/0/5
Ten-GigabitEthernet1/0/10
[Switch-vlan10] quit
```

Create a static MAC address entry for the server MAC address on Ten-GigabitEthernet 1/0/2.

```
[Switch] mac-address static 000f-e20f-dc71 interface Ten-GigabitEthernet 1/0/2 vlan 10
```

Set the MAC address learning limit to 0 on Ten-GigabitEthernet 1/0/10.

```
[Switch] interface Ten-GigabitEthernet 1/0/10
```

```
[Switch-Ten-GigabitEthernet1/0/10] mac-address max-mac-count 0
```

Configure a static MAC address entry for the NMS MAC address on the interface.

```
[Switch-Ten-GigabitEthernet1/0/10] mac-address static 0014-222c-aa69 vlan 10
```

Disable MAC address learning on Ten-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 Ten-GigabitEthernet 1/0/5
[Switch-Ten-GigabitEthernet1/0/5] undo mac-address mac-learning enable
[Switch-Ten-GigabitEthernet1/0/5] broadcast-suppression 50
[Switch-Ten-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 Ten-GigabitEthernet 1/0/5. Otherwise, broadcast storms might occur.

```
[Switch] interface Ten-GigabitEthernet 1/0/5
[Switch-Ten-GigabitEthernet1/0/5] mac-address mac-learning enable
[Switch-Ten-GigabitEthernet1/0/5] undo broadcast-suppression
[Switch-Ten-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Display the MAC address table configuration.

```
[Switch] display mac-address
MAC Address      VLAN ID    State           Port/NickName           Aging
00a0-fc00-583c    10        Blackhole       N/A                     N
000f-e20f-dc71    10        static          XGE 1/0/2               N
0014-222c-aa69    10        static          XGE 1/0/10              N
00e0-fc5e-b1fb    10        Learned         XGE 1/0/5               A
00e0-fc55-f116    10        Learned         XGE 1/0/5               A
0000-fc00-7507    10        Learned         XGE 1/0/5               A
0023-8927-aff0    10        Learned         XGE 1/0/5               A
0023-8927-b003    10        Learned         XGE 1/0/5               A
  ---  8 mac address(es) found  ---
```

Configuration files

```
#
vlan 10
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 10
 mac-address static 000f-e20f-dc71 vlan 10
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 10
#
```

```
interface Ten-GigabitEthernet1/0/10
 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

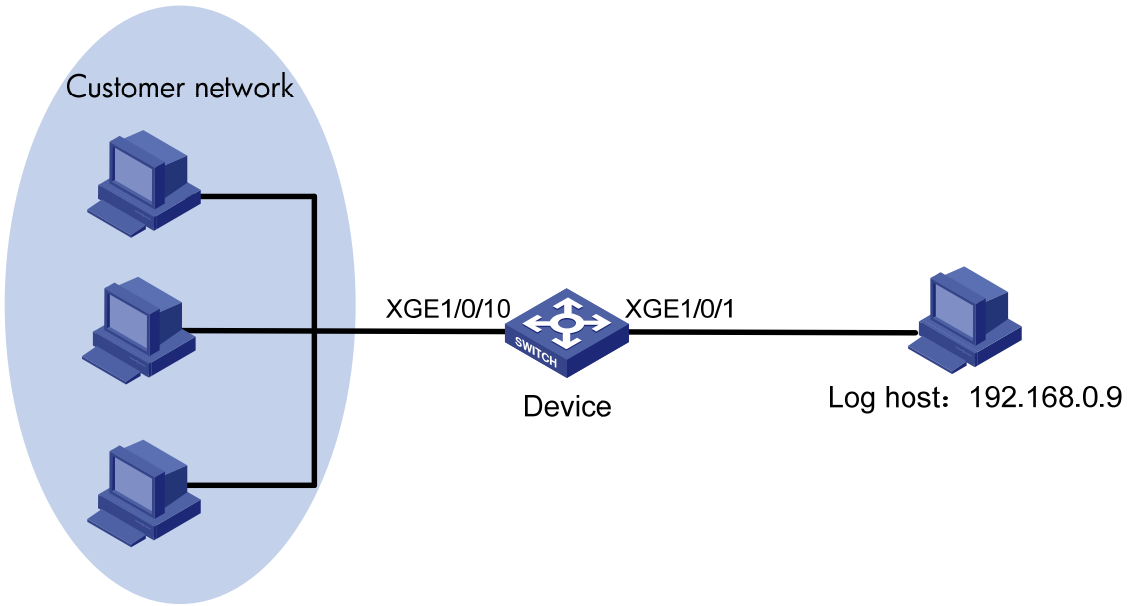
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 126, 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 126 Network diagram



Requirements analysis

To prevent syslog messages from being sent frequently, you must 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.
- The device records and sends the following MAC addresses:
  - Dynamic MAC addresses.
  - MAC addresses that pass MAC address authentication.
  - MAC addresses that pass 802.1X authentication.
  - Secure MAC addresses.
- The device does not record or send following MAC addresses:
  - Blackhole MAC addresses.
  - Static 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 Ten-GigabitEthernet 1/0/10.

   ```
   [Device] interface ten-gigabitethernet 1/0/10
   [Device-Ten-GigabitEthernet1/0/10] mac-address information enable added
   [Device-Ten-GigabitEthernet1/0/10] mac-address information enable deleted
   [Device-Ten-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. By default, the information center is enabled.

   ```
   [Device] info-center enable
   ```

   # Output syslog messages to the log host 192.168.0.9.

   ```
   [Device] info-center loghost 192.168.0.9
   ```

   # Output the MAC module's information with a severity level of at least informational to the log host.

   ```
   [Device] info-center source mac loghost level informational
   ```

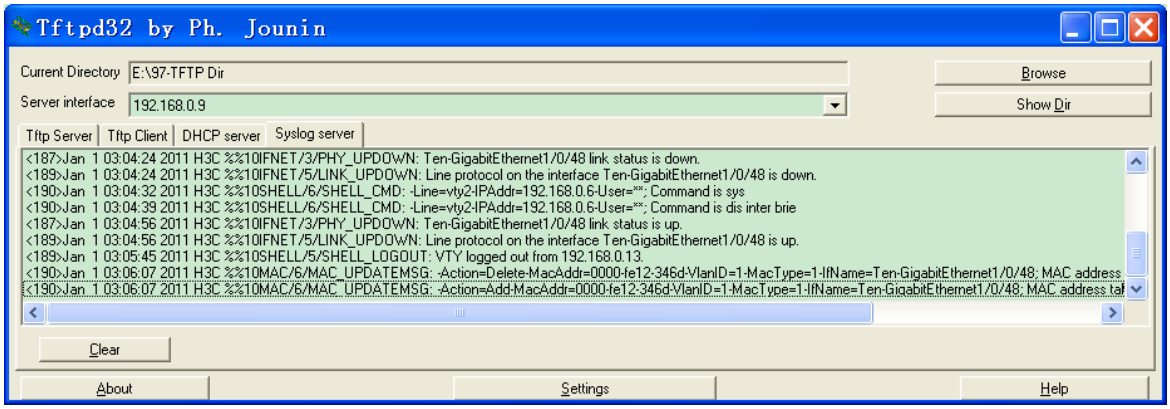
3. Run available applications that can receive log information on the log host (for example, IMC). (Details not shown.)

Verifying the configuration

Display MAC Information messages on the log host to verify the configuration.

In this example, the **tftpd32** tool in the log host can receive log information. The tool displays the log information as shown in Figure 127.

Figure 127 Log information



Configuration files

```
#
 mac-address information interval 300
 mac-address information mode syslog
 mac-address information enable
#
 info-center loghost 192.168.0.9
 info-center source MAC loghost level informational
#
interface Ten-GigabitEthernet1/0/10
 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

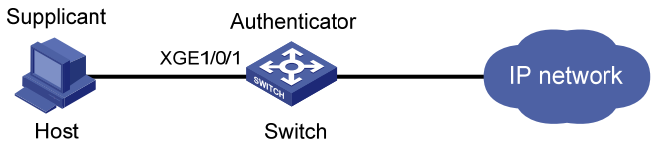
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 128:

- 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. The MAC addresses are hyphenated and in lower case.

Figure 128 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable MAC authentication on the access port, Ten-GigabitEthernet 1/0/1.
- Set correct MAC authentication timers to prevent continuous re-authentication of illegal MAC addresses.

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 has 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

Add a network access user account. Set both the username and password as the host's MAC address **68-05-ca-06-55-7b**.

```
<Switch> system-view
[Switch] local-user 68-05-ca-06-55-7b class network
New local user added.
[Switch-luser-network-68-05-ca-06-55-7b] password simple 68-05-ca-06-55-7b
```

Enable LAN access service for the account.

```
[Switch-luser-network-68-05-ca-06-55-7b] service-type lan-access
[Switch-luser-network-68-05-ca-06-55-7b] quit
```

Configure ISP domain **aabbcc.net** to perform local authentication for LAN 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. The switch detects whether a user has gone offline every 180 seconds.

```
[Switch] mac-authentication timer offline-detect 180
```

Set the MAC authentication quiet timer. If a user fails MAC authentication, the switch does not authenticate the user within 180 seconds.

```
[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 Ten-GigabitEthernet 1/0/1.

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] mac-authentication
[Switch-Ten-GigabitEthernet1/0/1] quit
```

Enable MAC authentication globally.

```
[Switch] mac-authentication
```

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
          Max number of users is 1024 per slot
          Current number of online users is 1
          Current authentication domain is aabbcc.net

Silent MAC User info:
          MAC Addr         VLAN ID  From Port                    Port Index


Ten-GigabitEthernet1/0/1 is link-up
  MAC authentication is enabled
  Max number of on-line users is 256
  Current number of online users is 1
  Current authentication domain: Not configured
Authenticate success: 1, failed: 364
         MAC Addr          Auth State
         6805-ca06-557b    authenticated
…
```

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
#
local-user 68-05-ca-06-55-7b class network
 password cipher $c$3$KEiYU/nrbJqmp75BldT4m99SzcSQ5Ro3sPRpTvUSd4aGL676
 service-type lan-access
authorization-attribute user-role network-operator
#
interface Ten-GigabitEthernet1/0/1
 mac-authentication
#
```

Example: Configuring RADIUS-based MAC authentication (MAC-based user account)

Applicable product matrix

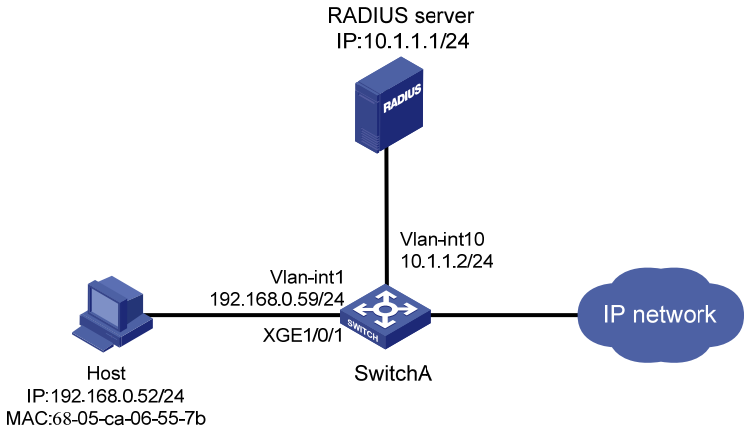
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 129:

- 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. The MAC addresses are hyphenated and in lower case.

Figure 129 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable MAC authentication on the access port, Ten-GigabitEthernet 1/0/1.
- Set correct MAC authentication timers to prevent continuous re-authentication of illegal MAC addresses.

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.
- Specify the authentication port as **1645** in the RADIUS scheme on the access device when an HP device functions as the RADIUS authentication server.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. The server runs the Comware V5 software image. 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 129. 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
New Radius scheme
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key simple 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 LAN 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 Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] mac-authentication
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain2
```

Set the MAC authentication offline detect timer. The switch detects whether a user has gone offline every 180 seconds.

```
[SwitchA] mac-authentication timer offline-detect 180
```

Set the MAC authentication quiet timer. If a user fails MAC authentication, the switch does not authenticate the user within 180 seconds.

```
[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
```

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
```

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 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
          Max number of users is 1024 per slot
          Current number of online users is 1
          Current authentication domain is domain2

Silent Mac User info:
         MAC Addr               VLAN ID  From Port           Port Index

Ten-Gigabitethernet1/0/1 is link-up
  MAC authentication is enabled
  Max number of online users is 256
  Current number of online users is 1
  Authentication attempts: successful 1, failed 0
          MAC Addr         Auth state
          6805-ca06-557b   authenticated
…
```

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
#
interface Ten-GigabitEthernet1/0/1
 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

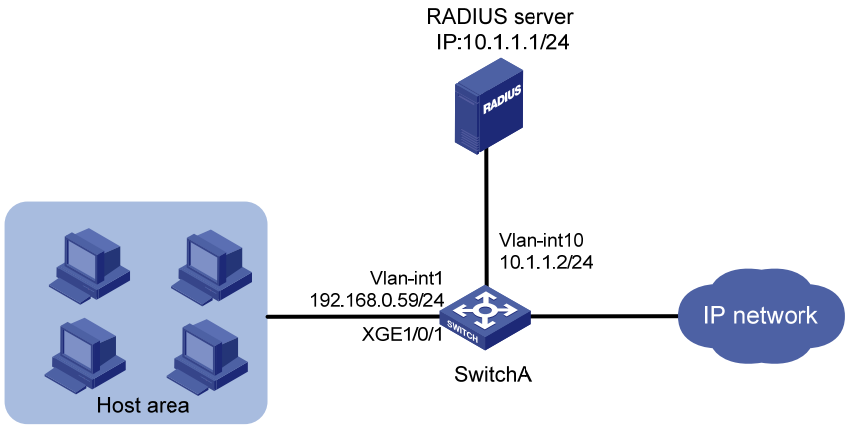
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 130:

- 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 130 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable MAC authentication on the access port, Ten-GigabitEthernet 1/0/1.
- Set correct MAC authentication timers to prevent continuous re-authentication of illegal MAC addresses.

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.
- Specify the authentication port as **1645** in the RADIUS scheme on the access device when an HP device functions as the RADIUS authentication server.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. The server runs the Comware V5 software image. 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 130. 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
New Radius scheme
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key simple 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 Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] mac-authentication
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain1
```

Set the MAC authentication offline detect timer. The switch detects whether a user has gone offline every 180 seconds.

```
[SwitchA] mac-authentication timer offline-detect 180
```

Set the MAC authentication quiet timer. If a user fails authentication, the switch does not authenticate the user within 180 seconds.

```
[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
```

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
```

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 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
          Max number of users is 1024 per slot
          Current number of online users is 4
          Current authentication domain is domain1

Silent Mac User info:
         MAC Addr               VLAN ID  From Port           Port Index

Ten-Gigabitethernet1/0/1 is link-up
  MAC authentication is enabled
  Max number of on-line users is 256
  Current number of online users is 4
  Current authentication domain: Not configured
  Authentication attempts: successful 4, failed 0
          MAC Addr         Auth state
          6805-ca06-557b   authenticated
          6805-ca00-8a11   authenticated
          6805-ca00-6677   authenticated
          6805-ca02-1122   authenticated

…
```

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
#
interface Ten-GigabitEthernet1/0/1
 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
#
```

MCE configuration examples

Introduction

This chapter provides examples for configuring the MCE to advertise VPN routes to the PE.

Example: Configuring the MCE to advertise VPN routes to the PE by using OSPF

Applicable product matrix

Product series	Software version
HP 5920	Release 2210
HP 5900	Release 2208P01

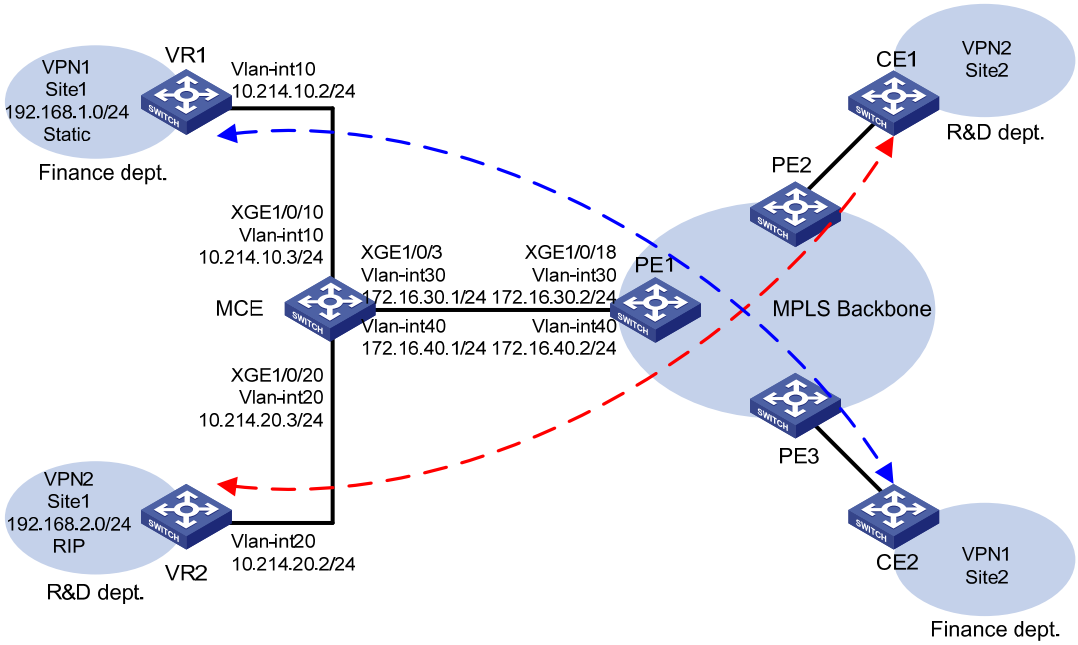
Network requirements

As shown in Figure 131, an enterprise has two MPLS L3VPNs connected over an MPLS backbone. VPN 1 for the finance department uses state routes, and VPN 2 for the R&D department uses RIP routes.

Configure the devices to meet the following requirements:

- The MCE can isolate the two VPNs by creating an independent routing table for each VPN.
- VPN sites can exchange VPN routes through PEs.

Figure 131 Network diagram

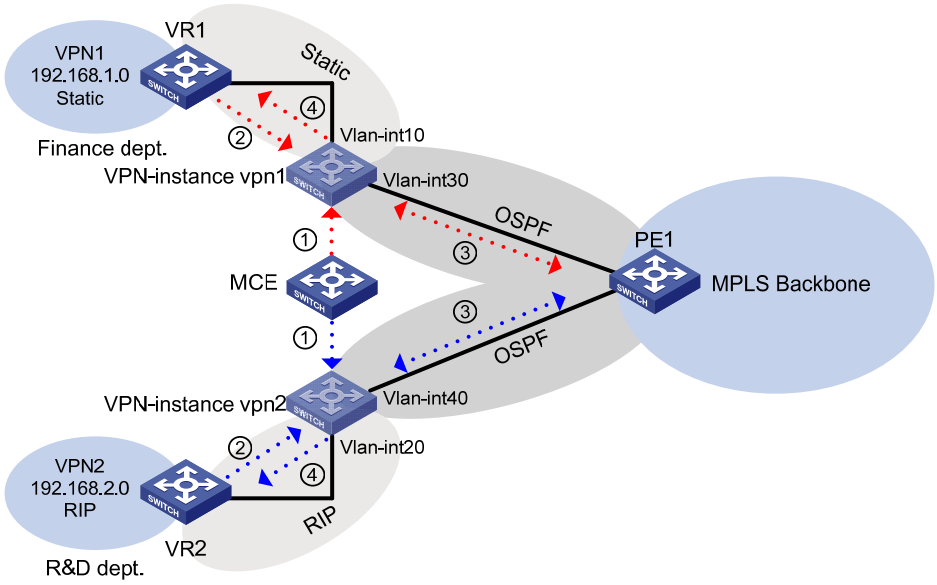


Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To isolate VPNs, you must create VPN instances on the MCE and PEs, and bind each VPN instance to the interfaces that need to forward data for that VPN instance. Figure 132 shows the order in which the MCE processes routing information for each VPN.
- For the VPN sites to exchange VPN routes, you must do the following:
  - Configure the VPN instances on the MCE to redistribute routes from VPN sites.
  - Advertise the VPN routes to the PE through OSPF.
  - Receive remote VPN routes from the PE.
  - Redistribute the remote VPN routes to the local VPN sites.

Figure 132 Network diagram



Configuration restrictions and guidelines

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

- After you execute the **ip binding vpn-instance** command on an interface, you must configure an IP address for that interface. The **ip binding vpn-instance** command removes the IP address of the bound interface.
- An OSPF process can belong to only one VPN instance, but a VPN instance can use multiple OSPF processes to advertise private routes. The OSPF processes in a VPN instance must have the same domain ID to ensure correct route advertisements.
- An OSPF process bound to a VPN instance does not use the public router ID configured in system view. You must configure a router ID for the OSPF process.

Configuration procedures

Configuring VPN instances on the MCE

Create VPN instance **vpn1**, and configure its RD as 10:1.

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] quit
```

Create VPN instance **vpn2**, and configure its RD as 20:1.

```
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] quit
```

Create VLAN 10, and assign Ten-GigabitEthernet 1/0/10 to VLAN 10.

```
[MCE] vlan 10
[MCE-vlan10] port ten-gigabitethernet 1/0/10
```

```
[MCE-vlan10] quit
```

Create VLAN-interface 10, and bind VLAN-interface 10 to VPN instance **vpn1**.

```
[MCE] interface Vlan-interface 10
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
```

Configure IP address 10.214.10.3/24 for the VLAN interface.

```
[MCE-Vlan-interface10] ip address 10.214.10.3 24
[MCE-Vlan-interface10] quit
```

Create VLAN 20, and assign Ten-GigabitEthernet 1/0/20 to VLAN 20.

```
[MCE] vlan 20
[MCE-vlan20] port ten-gigabitethernet 1/0/20
[MCE-vlan20] quit
```

Create VLAN-interface 20, and bind VLAN-interface 20 to VPN instance **vpn2**.

```
[MCE] interface Vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
```

Configure IP address 10.214.20.3/24 for the VLAN interface.

```
[MCE-Vlan-interface20] ip address 10.214.20.3 24
[MCE-Vlan-interface20] quit
```

Create VLAN 30 and VLAN 40.

```
[MCE] vlan 30
[MCE-vlan30] quit
[MCE] vlan 40
[MCE-vlan40] quit
```

Bind the trunk interface Ten-GigabitEthernet 1/0/3 to VLAN 30 and VLAN 40.

```
[MCE] interface ten-gigabitethernet 1/0/3
[MCE-Ten-GigabitEthernet1/0/3] port link-type trunk
[MCE-Ten-GigabitEthernet1/0/3] port trunk permit vlan 30 40
[MCE-Ten-GigabitEthernet1/0/3] quit
```

Do the following:

- Configure IP addresses for the VLAN interfaces.
- Bind VLAN 30 to VPN instance **vpn1**.
- Bind VLAN 40 to VPN instance **vpn2**.

```
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
[MCE-Vlan-interface30] ip address 172.16.30.1 24
[MCE-Vlan-interface30] quit
[MCE] interface Vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
[MCE-Vlan-interface40] ip address 172.16.40.1 24
[MCE-Vlan-interface40] quit
```

On PE 1:

- Configure the VPN instances and RDs.
- Bind VPN instances to the interface that connects to the MCE.

(Details not shown.)

To facilitate management, configure the same RD for a VPN instance on the MCE and PE.

Configuring routes to VPN sites for VPN instances

1. Configure a static route to VPN 1 site 1:

   # On VR 1:

   - Configure IP address 192.168.1.1/24 for the interface that connects to VPN 1 site 1.
   - Configure VLAN settings.

   (Details not shown.)

   # On VR 1, configure a default route with the next hop as the MCE.

```
<VR1> system-view
[VR1] ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

   # On the MCE:

   - Configure a static route destined for 192.168.1.0 through the next hop 10.214.10.2.
   - Bind the route to VPN instance **vpn1**.

```
[MCE] ip route-static vpn-instance vpn1 192.168.1.0 24 10.214.10.2
```

   # Display the routing table for VPN instance **vpn1**.

```
[MCE] display ip routing-table vpn-instance vpn1

Destinations : 7 Routes : 7

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.214.10.0/24      Direct 0    0           10.214.10.3     Vlan10
10.214.10.3/32      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
172.16.30.0/24      Direct 0    0           172.16.30.1     Vlan30
172.16.30.1/32      Direct 0    0           127.0.0.1       InLoop0
192.168.0.0/16      Static 60   0           10.214.10.2     Vlan10
```

   The output shows that the MCE has a static route to VPN 1 site 1.

2. Configure RIP to learn the route to VPN 2 site 1:

   # On VR 2, configure IP address 10.214.20.2/24 for the interface that connects to the MCE. (Details not shown.)

   # On VR 2, configure RIP process 20 to advertise networks 192.168.2.0 and 10.214.20.0.

```
<VR2> system-view
[VR2] rip 20
[VR2-rip-20] network 192.168.2.0
[VR2-rip-20] network 10.0.0.0
```

   # On the MCE, enable RIP process 20 for VPN instance **vpn2** to exchange routes with VPN 2 site 1.

```
[MCE] rip 20 vpn-instance vpn2
```

   # On the MCE, advertise the network 10.214.20.0, and disable route summarization.

```
[MCE-rip-20] network 10.0.0.0
[MCE-rip-20] undo summary
[MCE-rip-20] quit
```

   # Display the routing table for VPN instance **vpn2**.

```
[MCE] display ip routing-table vpn-instance vpn2

Destinations : 7 Routes : 7

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.214.20.0/24      Direct 0    0            10.214.20.3     Vlan20
10.214.20.3/32      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
172.16.40.0/30      Direct 0    0            172.16.40.1     Vlan40
172.16.40.1/32      Direct 0    0            127.0.0.1       InLoop0
192.168.2.0/24      RIP    100  1            10.214.20.2     Vlan20
```

The output shows that the MCE has learned a RIP route to VPN 2 site 1, which is in a different routing table from the static route to VPN 1 site 1. The routing information for different VPNs is separated.

Configuring route exchange between the MCE and PE 1

On PE 1, create VLAN 30 and VLAN 40.

```
<PE1> system-view
[PE1] vlan 30
[PE1-vlan30] quit
[PE1] vlan 40
[PE1-vlan40] quit
```

Assign Ten-GigabitEthernet1/0/18 to VLAN 30 and VLAN 40.

```
[PE1] interface ten-gigabitethernet 1/0/18
[PE1-Ten-GigabitEthernet1/0/18] port link-type trunk
[PE1-Ten-GigabitEthernet1/0/18] port trunk permit vlan 30 40
[PE1-Ten-GigabitEthernet1/0/18] undo port trunk permit vlan 1
[PE1-Ten-GigabitEthernet1/0/18] quit
```

On PE 1, create VPN instances **vpn1** and **vpn2** and their RDs, which are the same as those configured on the MCE.

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 10:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 20:1
[PE1-vpn-instance-vpn2] quit
```

On PE 1, configure IP addresses for VLAN-interface 30 and VLAN-interface 40, and bind the VLAN interfaces to VPN instances **vpn1** and **vpn2**, respectively.

```
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip binding vpn-instance vpn1
[PE1-Vlan-interface30] ip address 172.16.30.2 24
[PE1-Vlan-interface30] quit
[PE1-Vlan-interface40] ip binding vpn-instance vpn2
[PE1-Vlan-interface40] ip address 172.16.40.2 24
[PE1-Vlan-interface40] quit
```

Configure interface Loopback 0, and bind it to VPN instance **vpn1** on the MCE and PE, respectively.

```
[MCE] interface Loopback 0
[MCE-Loopback0] ip binding vpn-instance vpn1
[MCE-Loopback0] ip address 100.100.10.1 32
[MCE-Loopback0] quit
[PE1] interface Loopback 0
[PE1-Loopback0] ip binding-vpn-instance vpn1
[PE1-Loopback0] ip address 100.100.11.1 32
[PE1-Loopback0] quit
```

On the MCE:

- Enable OSPF process 10.
- Configure the IP address of Loopback 0 as the router ID.
- Bind OSPF process 10 to VPN instance **vpn1**.

```
[MCE] ospf 10 router-id 100.100.10.1 vpn-instance vpn1
```

On the MCE, enable VPN instance capability for OSPF process 10.

```
[MCE-ospf-10] vpn-instance-capability simple
```

On the MCE, advertise the network 172.16.30.0, and enable static route redistribution in area 0.

```
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 172.16.30.0 0.0.0.255
[MCE-ospf-10-area-0.0.0.0] quit
[MCE-ospf-10] import-route static
[MCE-ospf-10] quit
```

On PE 1:

- Enable OSPF process 10 for route exchange with the MCE.
- Configure the IP address of Loopback 0 as the router ID.
- Bind OSPF process 10 to VPN instance **vpn1**.

```
[PE1] ospf 10 router-id 100.100.11.1 vpn-instance vpn1
```

On PE 1, configure the domain ID as 10 for OSPF process 10.

```
[PE1-ospf-10] domain-id 10
```

On PE 1, enable VPN instance capability for OSPF process 10.

```
[PE1-ospf-10] vpn-instance-capability simple
```

On PE 1, advertise the network 172.16.30.0 in area 0.

```
[PE1-ospf-10] area 0
[PE1-ospf-10-area-0.0.0.0] network 172.16.30.0 0.0.0.255
[PE1-ospf-10-area-0.0.0.0] quit
[PE1-ospf-10] quit
```

Configure interface Loopback 1, and bind it to VPN instance **vpn2** on the MCE and PE, respectively.

```
[MCE] interface Loopback 1
[MCE-Loopback1] ip binding vpn-instance vpn2
[MCE-Loopback1] ip address 100.100.20.1 32
[MCE-Loopback1] quit
[PE1] interface Loopback 1
[PE1-Loopback1] ip binding-vpn-instance vpn2
[PE1-Loopback1] ip address 100.100.21.1 32
[PE1-Loopback1] quit
```

On the MCE:

- Enable OSPF process 20.
- Configure the IP address of Loopback 1 as the router ID.
- Bind OSPF process 10 to VPN instance **vpn2**.

```
[MCE] ospf 20 router-id 100.100.20.1 vpn-instance vpn2
```

On the MCE, enable VPN instance capability for OSPF process 10.

```
[MCE-ospf-20] vpn-instance-capability simple
```

Advertise the network 172.16.40.0, and enable RIP route redistribution in area 0.

```
[MCE-ospf-20] area 0
[MCE-ospf-20-area-0.0.0.0] network 172.16.40.0 0.0.0.255
[MCE-ospf-20-area-0.0.0.0] quit
[MCE-ospf-20] import-route rip
```

On PE 1:

- Enable OSPF process 20.
- Configure the IP address of Loopback 1 as the router ID.
- Bind OSPF process 10 to VPN instance **vpn2**.

```
[PE1] ospf 20 router-id 100.100.21.1 vpn-instance vpn2
```

Configure the domain ID as 20 for OSPF process 20.

```
[PE1-ospf-20] domain-id 20
```

Enable VPN instance capability for OSPF process 20.

```
[PE1-ospf-20] vpn-instance-capability simple
```

Advertise the network 172.16.40.0 in area 0.

```
[PE1-ospf-20] area 0
[PE1-ospf-20-area-0.0.0.0] network 172.16.40.0 0.0.0.255
[PE1-ospf-20-area-0.0.0.0] return
```

Verifying the configuration

Display the routing table for VPN instance **vpn1** on PE 1.

```
<PE1> display ip routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
100.100.11.1/32     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
172.16.30.0/24      Direct 0    0           172.16.30.2     Vlan30
172.16.30.2/32      Direct 0    0           127.0.0.1       InLoop0
192.168.1.0/24      O_ASE  150  1           172.16.30.1     Vlan30
```

The output shows that PE 1 has redistributed the route destined for VPN 1 site 1 into OSPF.

Display the routing table for VPN instance **vpn2** on PE 1.

```
<PE1> display ip routing-table vpn-instance vpn2
```

```
Destinations : 6 Routes : 6

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
100.100.21.1/32     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
172.16.40.0/24      Direct 0    0            172.16.40.2     Vlan40
172.16.40.2/32      Direct 0    0            127.0.0.1       InLoop0
192.168.10.0/24     O_ASE  150  1            172.16.40.1     Vlan40
```

The output shows that PE 1 has redistributed the route destined for VPN 2 site 2 into OSPF.

Configuration files

- MCE:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 100.100.10.1 255.255.255.255
#
interface LoopBack0
 ip binding vpn-instance vpn2
 ip address 100.100.20.1 255.255.255.255
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface20
 ip binding vpn-instance vpn2
 ip address 10.214.20.3 255.255.255.0
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.1 255.255.255.0
```

```
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 30 40
#
interface Ten-GigabitEthernet1/0/10
 port access vlan 10
#
interface Ten-GigabitEthernet1/0/20
 port access vlan 20
#
ospf 10 router-id 100.100.10.1 vpn-instance vpn1
 import-route static
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.30.0 0.0.0.255
#
ospf 20 router-id 100.100.20.1 vpn-instance vpn2
 import-route rip
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.40.0 0.0.0.255
#
rip 20 vpn-instance vpn2
 undo summary
 network 10.0.0.0
#
 ip route-static vpn-instance vpn1 192.168.1.0 255.255.255.0 10.214.10.2
```

- PE:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 100.100.11.1 255.255.255.255
#
```

```
interface LoopBack1
 ip binding vpn-instance vpn2
 ip address 100.100.21.1 255.255.255.255
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.2 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/18
 port link-type trunk
 port trunk permit vlan 30 40
#
ospf 10 router-id 100.100.10.1 vpn-instance vpn1
 domain-id 0.0.0.10
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.30.0 0.0.0.255
#
ospf 20 router-id 100.100.20.1 vpn-instance vpn2
 domain-id 0.0.0.20
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.40.0 0.0.0.255
```

Example: Configuring the MCE to advertise VPN routes to the PE by using BGP

Applicable product matrix

Product series	Software version
HP 5920	Release 2210
HP 5900	Release 2208P01

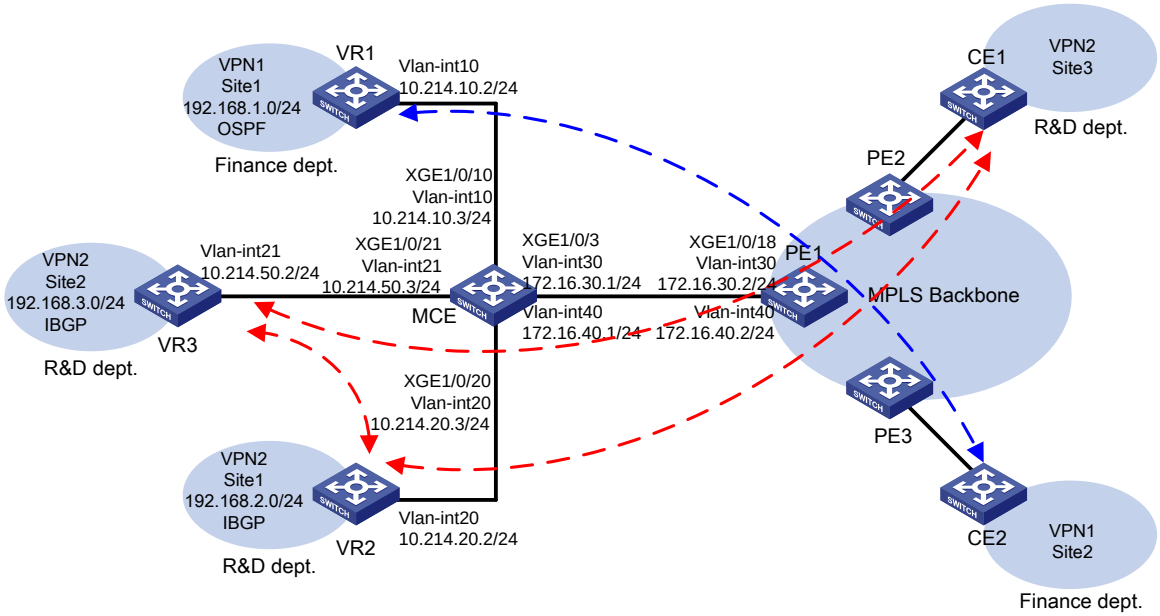
Network requirements

As shown in Figure 133, an enterprise has two MPLS L3VPNs connected over an MPLS backbone. VPN 1 for the finance department uses OSPF, and VPN 2 for the R&D department uses IBGP.

Configure the devices to meet the following requirements:

- The MCE can isolate the two VPNs by creating an independent routing table for each VPN.
- VPN sites can exchange VPN routes through PEs.

Figure 133 Network diagram

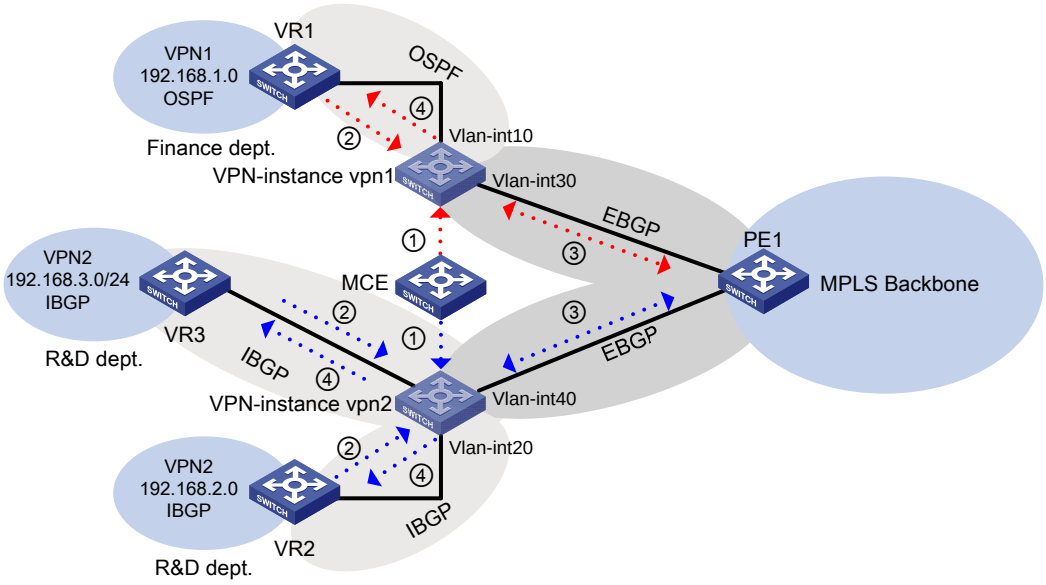


Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To isolate VPNs, you must create VPN instances on the MCE and PEs, and bind each VPN instance to the interfaces that need to forward data for that VPN instance. Figure 134 shows the order in which the MCE processes routing information for each VPN.
- For the VPN sites to exchange VPN routes, you must do the following:
  - Configure the VPN instances on the MCE to redistribute routes from VPN sites.
  - Advertise the VPN routes to the PE through EBGP.
  - Receive remote VPN routes from the PE.
  - Redistribute the remote VPN routes to the local VPN sites.
- IBGP requires a fully meshed network or a router reflector. In this example, you must configure the MCE as the IBGP route reflector.

Figure 134 Network diagram



Configuration restrictions and guidelines

After you execute the **ip binding vpn-instance** command on an interface, you must configure an IP address for that interface. The **ip binding vpn-instance** command removes the IP address of the bound interface.

Configuration procedures

Configuring VPN instances on the MCE

Create VPN instance **vpn1**, and configure its RD as 10:1.

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] quit
```

Create VPN instance **vpn2**, and configure its RD as 20:1.

```
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] quit
```

Create VLAN 10, and assign Ten-GigabitEthernet 1/0/10 to VLAN 10.

```
[MCE] vlan 10
[MCE-vlan10] port ten-gigabitethernet 1/0/10
[MCE-vlan10] quit
```

Create VLAN-interface 10, and bind VLAN-interface 10 to VPN instance **vpn1**.

```
[MCE] interface Vlan-interface 10
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
```

Configure IP address 10.214.10.3/24 for the VLAN interface.

```
[MCE-Vlan-interface10] ip address 10.214.10.3 24
```

```
[MCE-Vlan-interface10] quit
```

Create VLAN 20, and assign Ten-GigabitEthernet 1/0/20 to VLAN 20.

```
[MCE] vlan 20
[MCE-vlan20] port ten-gigabitethernet 1/0/20
[MCE-vlan20] quit
```

Create VLAN-interface 20, and bind VLAN-interface 20 to VPN instance **vpn2**.

```
[MCE] interface Vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
```

Configure IP address 10.214.20.3/24 for the VLAN interface.

```
[MCE-Vlan-interface20] ip address 10.214.20.3 24
[MCE-Vlan-interface20] quit
```

Create VLAN 21, and assign Ten-GigabitEthernet 1/0/21 to VLAN 21.

```
[MCE] vlan 21
[MCE-vlan21] port ten-gigabitethernet 1/0/21
[MCE-vlan21] quit
```

Create VLAN-interface 21, and bind VLAN-interface 21 to VPN instance **vpn2**.

```
[MCE] interface Vlan-interface 21
[MCE-Vlan-interface21] ip binding vpn-instance vpn2
```

Configure IP address 10.214.50.3/24 for the VLAN interface.

```
[MCE-Vlan-interface21] ip address 10.214.50.3 24
[MCE-Vlan-interface21] quit
```

Create VLAN 30 and VLAN 40.

```
[MCE] vlan 30
[MCE-vlan30] quit
[MCE] vlan 40
[MCE-vlan40] quit
```

Bind the trunk interface Ten-GigabitEthernet 1/0/3 to VLAN 30 and VLAN 40.

```
[MCE] interface ten-gigabitethernet 1/0/3
[MCE-Ten-GigabitEthernet1/0/3] port link-type trunk
[MCE-Ten-GigabitEthernet1/0/3] port trunk permit vlan 30 40
[MCE-Ten-GigabitEthernet1/0/3] quit
```

Do the following:

- Configure IP addresses for the VLAN interfaces.
- Bind VLAN 30 to VPN instance **vpn1**.
- Bind VLAN 40 to VPN instance **vpn2**.

```
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
[MCE-Vlan-interface30] ip address 172.16.30.1 24
[MCE-Vlan-interface30] quit
[MCE] interface Vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
[MCE-Vlan-interface40] ip address 172.16.40.1 24
[MCE-Vlan-interface40] quit
```

On PE 1:

- Configure the VPN instances and RDs.
- Bind VPN instances to the interface that connects to the MCE.

(Details not shown.)

To facilitate management, configure the same RD for a VPN instance on the MCE and PE 1.

Configuring routes destined to VPN sites for VPN instances

1. Configure OSPF to learn the route to VPN 1 site 1.

On VR 1:

- Configure IP address 192.168.1.1/24 for the interface that connects to VPN 1 site 1.
- Configure VLAN settings.

(Details not shown.)

On VR 1, enable OSPF, and advertise networks 192.168.1.0/24 and 10.214.10.2/24.

```
<VR1> system-view
[VR1] ospf
[VR1-ospf-1] area 0
[VR1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[VR1-ospf-1-area-0.0.0.0] network 10.214.10.0 0.0.0.255
```

On the MCE:

- Configure IP address 101.101.10.1 for interface Loopback 0.
- Bind Loopback 0 to VPN instance **vpn1**.

```
[MCE] interface loopback 0
[MCE--LoopBack0] ip binding vpn-instance vpn1
[MCE--LoopBack0] ip address 101.101.10.1 32
[MCE--LoopBack0] quit
```

On the MCE:

- Cnable OSPF process 1.
- Bind it to VPN instance **vpn1**.
- Specify the IP address of Loopback 0 as the router ID.

```
[MCE] ospf 1 vpn-instance vpn1 router-id 101.101.10.1
```

On the MCE, advertise network 10.214.10.0.

```
[MCE-ospf-1] area 0
[MCE-ospf-1-area-0.0.0.0] network 10.214.10.0 0.0.0.255
[MCE-ospf-1-area-0.0.0.0] quit
[MCE-ospf-1] quit
```

Display the routing table for VPN instance **vpn1** on the MCE.

```
[MCE] display ip routing-table vpn-instance vpn1

Destinations : 5 Routes : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
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
10.214.10.0/24      Direct 0     0           10.214.10.3     Vlan10
10.214.10.3/32      Direct 0     0           127.0.0.1       InLoop0
192.168.1.0/24      OSPF   10    2           10.214.10.2     Vlan10
```

The output shows that the MCE has learned an OSPF route to VPN 1 site 1.

2. Configure BGP to learn the routes to VPN 2 sites.

   # On VR 2, configure IP address 10.214.20.2 for the interface that connects to the MCE. (Details not shown.)

   # On VR 3, configure IP address 10.214.50.2 for the interface that connects to the MCE. (Details not shown.)

   # On the MCE:

   - Configure IP address 10.214.20.3 for the interface that connects to the VR 2.
   - Configure IP address 10.214.50.3 for the interface that connects to VR 3.

   (Details not shown.)

   # On VR 2:

   - Enable BGP in AS 100, specify the MCE at 10.214.20.3 as a BGP peer.
   - Advertise networks 192.168.2.0 and 10.214.20.0.

```
<VR2> system-view
[VR2] bgp 100
[VR2-bgp] router-id 2.2.2.2
[VR2-bgp] peer 10.214.20.3 as-number 100
[VR2-bgp] ipv4-family
[VR2-bgp-ipv4] peer 10.214.20.3 enable
[VR2-bgp-ipv4] network 192.168.2.0 24
[VR2-bgp-ipv4] network 10.214.20.0 24
```

   # On VR 3:

   - Enable BGP in AS 100.
   - Specify the MCE as a BGP peer.
   - Advertise networks 192.168.2.0 and 10.214.20.0.

```
<VR3> system-view
[VR3] bgp 100
[VR3-bgp] router-id 3.3.3.3
[VR3-bgp] peer 10.214.50.3 as-number 100
[VR3-bgp] ipv4-family
[VR3-bgp-ipv4] peer 10.214.50.3 enable
[VR3-bgp-ipv4] network 192.168.3.0 24
[VR3-bgp-ipv4] network 10.214.50.0 24
[VR3-bgp-ipv4] network 3.3.3.3 32
```

   # On the MCE:

   - Enable BGP in AS 100.
   - Create BGP-VPN instance **vpn2**.
   - Specify BGP peers 10.214.20.2 and 10.214.50.2.
   - Advertise networks 10.214.20.0/24 and 10.214.50.0/24.

```
[MCE] bgp 100
[MCE-bgp] ip vpn-instance vpn2
[MCE-bgp-vpn2] peer 10.214.20.2 as-number 100
[MCE-bgp-vpn2] peer 10.214.50.2 as-number 100
[MCE-bgp-vpn2] ipv4-family
```

```
[MCE-bgp-ipv4-vpn2] peer 10.214.20.2 enable
[MCE-bgp-ipv4-vpn2] peer 10.214.50.2 enable
[MCE-bgp-ipv4-vpn2] network 10.214.20.0 24
[MCE-bgp-ipv4-vpn2] network 10.214.50.0 24
```

Configure the MCE as a router reflector. Configure VR 2 and VR 3 as its clients.

```
[MCE-bgp-ipv4-vpn2] peer 10.214.20.2 reflect-client
[MCE-bgp-ipv4-vpn2] peer 10.214.50.2 reflect-client
[MCE-bgp-ipv4-vpn2] quit
[MCE-bgp-vpn2] quit
```

Display the BGP routing table on the MCE.

```
[MCE-bgp] display bgp routing-table ipv4

 Total number of routes: 3

 BGP Local router ID is 4.4.4.4
 Status codes: * - valid, > - best, d - damped, h - history,
               s - suppressed, S - Stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

*  i 192.168.2.0/24     10.214.20.2     0          100        0       i
*  i 192.168.3.0/24     10.214.50.2     0          100        0       i
* >  10.214.20.0/24     0.0.0.0         0                     0       i
* >  10.214.50.0/24     0.0.0.0         0                     0       i
```

The output shows that the MCE has learned BGP routes to VPN 2 sites.

Configuring route exchange between the MCE and PE 1

On PE 1, add Ten-GigabitEthernet 1/0/18 to VLAN 30 and VLAN 40.

```
<PE1> system-view
[PE1] interface ten-gigabitethernet 1/0/18
[PE1-Ten-GigabitEthernet1/0/18] port link-type trunk
[PE1-Ten-GigabitEthernet1/0/18] port trunk permit vlan 30 40
[PE1-Ten-GigabitEthernet1/0/18] quit
```

On PE 1, configure IP addresses for VLAN interfaces 30 and 40, and bind the VLAN interfaces to VPN instances **vpn1** and **vpn2**, respectively.

```
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip binding vpn-instance vpn1
[PE1-Vlan-interface30] ip address 172.16.30.2 24
[PE1-Vlan-interface30] quit
[PE1] interface vlan-interface 40
[PE1-Vlan-interface40] ip binding vpn-instance vpn2
[PE1-Vlan-interface40] ip address 172.16.40.2 24
[PE1-Vlan-interface40] quit
```

Enable BGP in AS 200, and create BGP-VPN instances **vpn1** and **vpn2**.

```
[PE1] bgp 200
[PE1-bgp] ip vpn-instance vpn1
```

```
[PE1-bgp-vpn1] quit
[PE1-bgp] ip vpn-instance vpn2
[PE1-bgp-vpn2] quit
```

On the MCE:

- Create BGP-VPN instance **vpn1**.
- Redistribute OSPF routes for **vpn1**.

```
[MCE-bgp] ip vpn-instance vpn1
[MCE-bgp-vpn1] ipv4-family
[MCE-bgp-ipv4-vpn1] import-route ospf
[MCE-bgp-ipv4-vpn1] quit
```

On the MCE:

- Specify PE 1 as an EBGP peer in AS 200.
- Advertise network 172.16.30.0 for BGP-VPN instance **vpn1**.

```
[MCE-bgp-vpn1] peer 172.16.30.2 as-number 200
[MCE-bgp-vpn1] ipv4-family
[MCE-bgp-ipv4-vpn1] peer 172.16.30.2 enable
[MCE-bgp-ipv4-vpn1] network 172.16.30.0 24
[MCE-bgp-ipv4-vpn1] quit
[MCE-bgp-vpn1] quit
```

On PE 1:

- Specify the MCE as an EBGP peer in AS 100.
- Advertise network 172.16.30.0 for BGP-VPN instance **vpn1**.

```
[PE1-bgp] ip vpn-instance vpn1
[PE1-bgp-vpn1] peer 172.16.30.1 as-number 100
[PE1-bgp-vpn1] ipv4-family
[PE1-bgp-ipv4-vpn1] peer 172.16.30.1 enable
[PE1-bgp-ipv4-vpn1] network 172.16.30.0 24
[PE1-bgp-ipv4-vpn1] quit
[PE1-bgp-vpn1] quit
```

On the MCE:

- Specify EBGP peer 172.16.40.2 in AS 200.
- Advertise network 172.16.40.0 for BGP-VPN instance **vpn2**.

```
[MCE-bgp] ip vpn-instance vpn2
[MCE-bgp-vpn2] peer 172.16.40.2 as-number 200
[MCE-bgp-vpn2] ipv4-family
[MCE-bgp-ipv4-vpn2] peer 172.16.40.2 enable
[MCE-bgp-ipv4-vpn2] network 172.16.40.0 24
[MCE-bgp-ipv4-vpn2] return
```

On PE 1:

- Specify EBGP peer 172.16.40.1 in AS 100.
- Advertise network 172.16.40.0 for BGP-VPN instance **vpn2**.

```
[PE1-bgp] ip vpn-instance vpn2
[PE1-bgp-vpn2] peer 172.16.40.1 as-number 100
[PE1-bgp-vpn2] ipv4-family
```

```
[PE1-bgp-ipv4-vpn2] peer 172.16.40.2 enable
[PE1-bgp-ipv4-vpn2] network 172.16.40.0 24
[PE1-bgp-ipv4-vpn2] return
```

Verifying the configuration

On the MCE, display EBGP peers for VPN instance **vpn1**.

```
<MCE> display bgp peer ipv4 vpn-instance vpn1

 BGP local router ID : 172.16.40.1
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  172.16.30.2             200       18       21    0       1 00:16:25 Established
```

The output shows that the MCE has an EBGP peer PE 1.

On PE 1, display the routing table for VPN instance **vpn1**.

```
<PE1> display ip routing-table vpn-instance vpn1

Destinations : 5 Routes : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

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
172.16.30.0/24      Direct 0    0            172.16.30.2     Vlan30
172.16.30.2/24      Direct 0    0            127.0.0.1       InLoop0
192.168.1.0/24      BGP    255  3            172.16.30.1     Vlan30
```

The output shows that VPN instance **vpn1** has learned a BGP route to VPN 1 site 1.

On the MCE, display EBGP peers for VPN instance **vpn2**.

```
<MCE> display bgp peer ipv4 vpn-instance vpn2

 BGP local router ID : 172.16.40.1
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  172.16.40.2             200       18       21    0       1 00:16:25 Established
```

The output shows that the MCE has an EBGP peer PE 1.

On PE 1, display the routing table for VPN instance **vpn2**.

```
<PE1> display ip routing-table vpn-instance vpn2

Destinations : 5 Routes : 5
```

```
Destination/Mask    Proto  Pre  Cost        NextHop         Interface

10.214.20.0/24      BGP    255  0           172.16.40.1     Vlan30
10.214.50.0/24      BGP    255  0           172.16.40.1     Vlan30
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
172.16.40.0/24      Direct 0    0           172.16.40.2     Vlan40
172.16.40.2/24      Direct 0    0           127.0.0.1       InLoop0
192.168.2.0/24      BGP    255  0           172.16.40.1     Vlan30
192.168.3.0/24      BGP    255  0           172.16.40.1     Vlan30
```

The output shows that VPN instance **vpn2** has learned BGP routes to VPN 2 sites.

Configuration files

- MCE:

```
#
vlan 10
#
vlan 20 to 21
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 101.101.10.1 255.255.255.255
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface20
 ip binding vpn-instance vpn2
 ip address 10.214.20.3 255.255.255.0
#
interface Vlan-interface21
 ip binding vpn-instance vpn2
 ip address 10.214.50.3 255.255.255.0
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.1 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.1 255.255.255.0
#
```

```
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 30 40
#
interface Ten-GigabitEthernet1/0/10
 port access vlan 10
#
interface Ten-GigabitEthernet1/0/20
 port access vlan 20
#
interface Ten-GigabitEthernet1/0/21
 port access vlan 21
#
bgp 100
 #
 ip vpn-instance vpn1
  peer 172.16.30.2 as-number 200
  #
  ipv4-family unicast
   import-route ospf 1
   network 172.16.30.0 255.255.255.0
   peer 172.16.30.2 enable
 #
 ip vpn-instance vpn2
  peer 10.214.20.2 as-number 100
  peer 10.214.50.2 as-number 100
  peer 172.16.40.2 as-number 200
  #
  ipv4-family unicast
   network 10.214.20.0 255.255.255.0
   network 10.214.50.0 255.255.255.0
   network 172.16.40.0 255.255.255.0
   peer 10.214.20.2 enable
   peer 10.214.20.2 reflect-client
   peer 10.214.50.2 enable
   peer 10.214.50.2 reflect-client
   peer 172.16.40.2 enable
#
ospf 1 router-id 101.101.10.1 vpn-instance vpn1
 area 0.0.0.0
  network 10.214.10.0 0.0.0.255
#
```

- PE 1:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
```

```
 route-distinguisher 20:1
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 100.100.11.1 255.255.255.255
#
interface LoopBack1
 ip binding vpn-instance vpn2
 ip address 100.100.21.1 255.255.255.255
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.2 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/18
 port link-type trunk
 port trunk permit vlan 30 40
#
bgp 200
 #
 ip vpn-instance vpn1
  peer 172.16.30.1 as-number 100
  #
  ipv4-family unicast
   network 172.16.30.0 255.255.255.0
   peer 172.16.30.1 enable
 #
 ip vpn-instance vpn2
  peer 172.16.40.1 as-number 100
  #
  ipv4-family unicast
   network 172.16.40.0 255.255.255.0
   peer 172.16.40.1 enable
#
```

Mirroring configuration examples

This document provides mirroring configuration examples.

Table 15 Mirroring types and application 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.
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 through which traffic to be monitored passes is not directly connected to the data monitoring device.

Example: Configuring local port mirroring

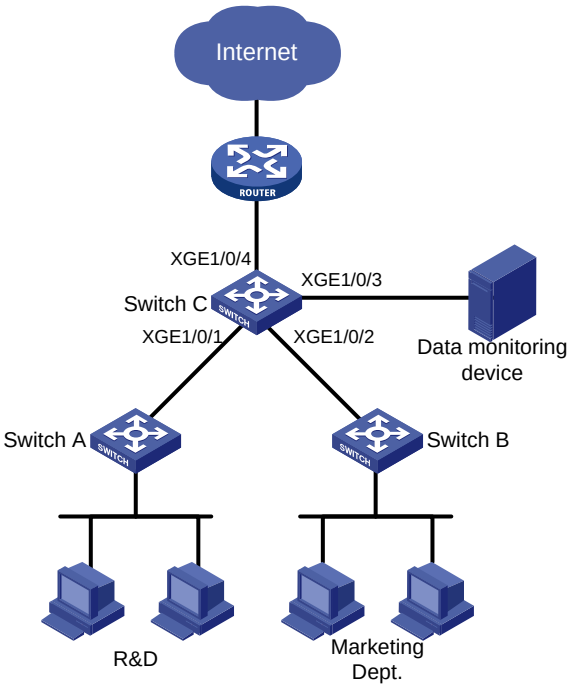
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 135, configure local port mirroring to monitor the Internet traffic and bidirectional traffic of the Marketing Department and the R&D Department.

Figure 135 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 as the source ports of the mirroring group. Configure the mirroring group to monitor the incoming traffic of the ports.

```
[SwitchC] mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/1 Ten-GigabitEthernet 1/0/2 inbound
```

Configure Ten-GigabitEthernet 1/0/3 as the monitor port of the mirroring group.

```
[SwitchC] mirroring-group 1 monitor-port Ten-GigabitEthernet 1/0/3
```

Disable the spanning tree feature on Ten-GigabitEthernet 1/0/3 to make sure mirroring operates correctly.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] undo stp enable
```

```
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        Ten-GigabitEthernet1/0/1  Inbound
        Ten-GigabitEthernet1/0/2  Inbound
    Monitor port: Ten-GigabitEthernet1/0/3
```

Configuration files

```
#
 mirroring-group 1 local
#
interface Ten-GigabitEthernet1/0/1
 mirroring-group 1 mirroring-port inbound
#
interface Ten-GigabitEthernet1/0/2
 mirroring-group 1 mirroring-port inbound
#
interface Ten-GigabitEthernet1/0/3
 undo stp enable
 mirroring-group 1 monitor-port
#
```

Example: Configuring Layer 2 remote port mirroring

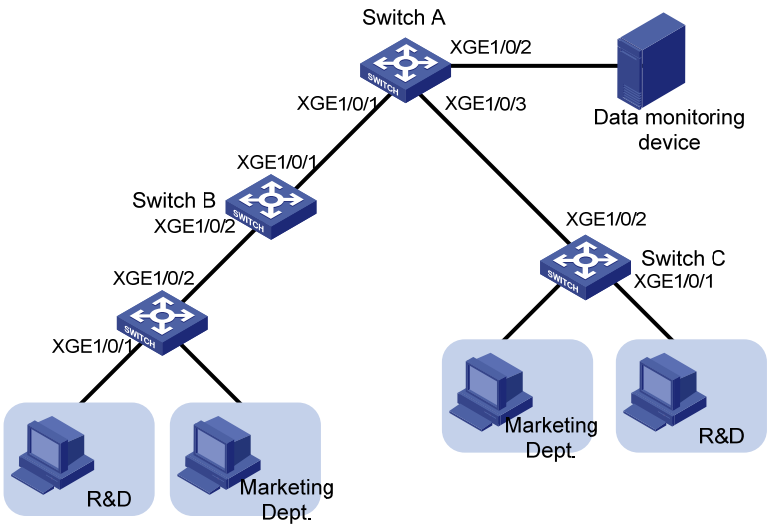
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 136, configure Layer 2 remote port mirroring to monitor the outgoing traffic of the R&D Departments.

Figure 136 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/3 as trunk ports to permit the packets from VLAN 2 to pass through.

```
<SwitchA> system-view
[SwitchA] interface Ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 2
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Create a remote destination group.

```
[SwitchA] mirroring-group 1 remote-destination
```

Create VLAN 2.

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

Configure VLAN 2 as the remote probe VLAN in the mirroring group.

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
```

Configure Ten-GigabitEthernet 1/0/2 as the monitor port in the mirroring group.

```
[SwitchA] mirroring-group 1 monitor-port Ten-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 Ten-GigabitEthernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port access vlan 2
```

Disable the spanning tree feature on Ten-GigabitEthernet 1/0/2 to make sure mirroring operates correctly.

```
[SwitchC-Ten-GigabitEthernet1/0/2] undo stp enable
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch B (the intermediate device)

Create VLAN 2.

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

Configure Ten-GigabitEthernet 1/0/1 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 2
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch C (the source device)

Create a remote source group.

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 remote-source
```

Create VLAN 2.

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

Configure VLAN 2 as the remote probe VLAN of remote source group 1.

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
```

Configure Ten-GigabitEthernet 1/0/1 as the source port of remote source group 1. Configure the mirroring group to monitor the incoming traffic of Ten-GigabitEthernet 1/0/1.

```
[SwitchC] mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/1 inbound
```

Configure Ten-GigabitEthernet 1/0/2 as the egress port of remote source group 1.

```
[SwitchC] mirroring-group 1 monitor-egress Ten-GigabitEthernet 1/0/2
```

Configure Ten-GigabitEthernet 1/0/2 as a trunk port to permit the packets from VLAN 2 to pass through.

```
[SwitchC] interface Ten-GigabitEthernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 2
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Disable the spanning tree and MAC address learning features on Ten-GigabitEthernet 1/0/2 to make sure mirroring operates correctly.

```
[SwitchC-Ten-GigabitEthernet1/0/2] undo stp enable
[SwitchC-Ten-GigabitEthernet1/0/2] undo mac-address mac-learning enable
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch D (the source device)

Configure Switch D in the same way that Switch C is configured. (Details are not shown.)

Verifying the configuration

Display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        Ten-GigabitEthernet1/0/1  Inbound
    Monitor egress port: Ten-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: Ten-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 Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
 undo stp enable
 mirroring-group 1 monitor-port
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 to 2
```

- Switch B:

```
#
vlan 2
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface Ten-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 Ten-GigabitEthernet1/0/1
 mirroring-group 1 mirroring-port inbound
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
```

```
 port trunk permit vlan 1 to 2
 undo stp enable
 undo mac-address mac-learning enable
 mirroring-group 1 monitor-egress
#
```

Example: Configuring local traffic mirroring

Applicable product matrix

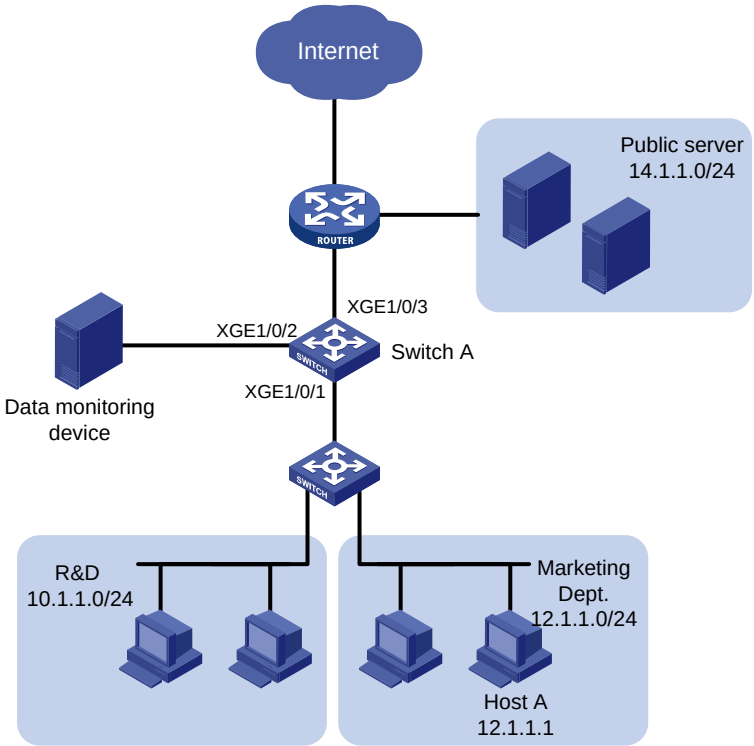
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 137, configure local traffic mirroring to mirror the following traffic:

- HTTP traffic sent by the R&D 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 137 Network diagram



Configuration procedures

1. Configure a QoS policy that mirrors Internet traffic from the R&D Department:

   # Create ACL 3000.

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

   # Configure a rule to permit packets from the R&D Department to access the Internet.

   ```
   [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 Ten-GigabitEthernet 1/0/2.

   ```
   [SwitchA] traffic behavior behavior_research
   [SwitchA-behavior-behavior_research] mirror-to interface Ten-GigabitEthernet 1/0/2
   [SwitchA-behavior-behavior_research] quit
   ```

   # Create QoS policy **policy_research**.

   ```
   [SwitchA] qos policy policy_research
   ```

   # Associate traffic class **classifier_research** with traffic behavior **behavior_research** in the QoS policy.

   ```
   [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.

   ```
   [SwitchA] acl number 3001
   ```

   # Configure two rules to permit packets from the public server to Host A during non-working hours on working days.

   ```
   [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 Ten-GigabitEthernet 1/0/2.

```
[SwitchA] traffic behavior behavior_market
[SwitchA-behavior-behavior_market] mirror-to interface Ten-GigabitEthernet 1/0/2
[SwitchA-behavior-behavior_market] quit
```

Create QoS policy **policy_market**.

```
[SwitchA] qos policy policy_market
```

Associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[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 Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy policy_research inbound
```

Apply QoS policy **policy_market** to the outgoing packets of Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy policy_market outbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display local traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface Ten-GigabitEthernet 1/0/1

  Interface: Ten-GigabitEthernet1/0/1

  Direction: Inbound

  Policy: policy_research
   Classifier: classifier_research
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: behavior_research
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/2

  Direction: Outbound

  Policy: policy_market
   Classifier: classifier_market
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: behavior_market
      Mirroring:
        Mirror to the interface: Ten-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 Ten-GigabitEthernet1/0/2
traffic behavior behavior_market
 mirror-to interface Ten-GigabitEthernet1/0/2
#
qos policy policy_research
 classifier classifier_research behavior behavior_research
qos policy policy_market
 classifier classifier_market behavior behavior_market
#
interface Ten-GigabitEthernet1/0/1
 qos apply policy policy_research inbound
 qos apply policy policy_market outbound
```

Example: Configuring remote traffic mirroring

Applicable product matrix

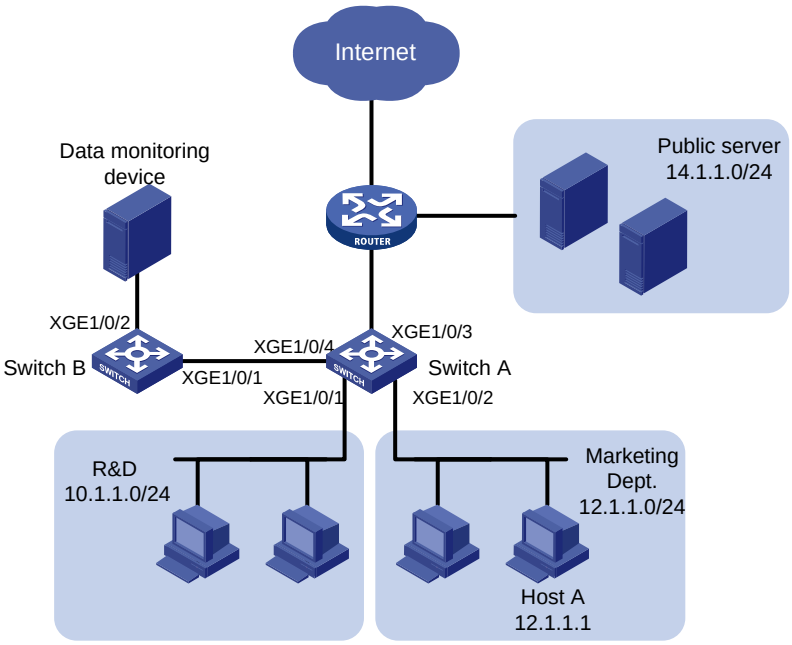
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 138, configure remote traffic mirroring to mirror the following traffic:

- HTTP traffic sent by the R&D 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 138 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.

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

Configure a rule to permit packets from the R&D Department to access the Internet.

```
[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 Ten-GigabitEthernet 1/0/4.

```
[SwitchA] traffic behavior behavior_research
[SwitchA-behavior-behavior_research] mirror-to interface Ten-GigabitEthernet 1/0/4
[SwitchA-behavior-behavior_research] quit
```

Create QoS policy **policy_research**.

```
[SwitchA] qos policy policy_research
```

Associate traffic class **classifier_research** with traffic behavior **behavior_research** in the QoS policy.

```
[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.

```
[SwitchA] acl number 3001
```

Configure two rules to permit packets from the public server to Host A during non-working hours on working days.

```
[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 Ten-GigabitEthernet 1/0/4.

```
[SwitchA] traffic behavior behavior_market
[SwitchA-behavior-behavior_market] mirror-to interface Ten-GigabitEthernet 1/0/4
[SwitchA-behavior-behavior_market] quit
```

Create QoS policy **policy_market**.

```
[SwitchA] qos policy policy_market
```

Associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[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 Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy policy_research inbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Apply QoS policy **policy_market** to the outgoing packets of Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy policy_market outbound
[SwitchA-Ten-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 (Ten-GigabitEthernet 1/0/10, in this example) as a source port of remote source group 1.

```
[SwitchA] mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/10 inbound
```

Configure Ten-GigabitEthernet 1/0/4 as the egress port of remote source group 1.

```
[SwitchA] mirroring-group 1 monitor-egress Ten-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 Ten-GigabitEthernet 1/0/4 as a trunk port.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] port link-type trunk
```

Assign the port Ten-GigabitEthernet 1/0/4 to VLAN 2.

```
[SwitchA-Ten-GigabitEthernet1/0/4] port trunk permit vlan 2
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

Configuring Switch B

Configure Ten-GigabitEthernet 1/0/1 as a trunk port.

```
<SwitchB> system-view
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port Ten-GigabitEthernet 1/0/1 to VLAN 2.

```
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-Ten-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 Ten-GigabitEthernet 1/0/2 as the monitor port of the remote destination group.

```
[SwitchB] mirroring-group 1 monitor-port Ten-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 Ten-GigabitEthernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port access vlan 2
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display remote traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface

  Interface: Ten-GigabitEthernet1/0/1
```

```
  Direction: Inbound

  Policy: policy_research
   Classifier: classifier_research
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: behavior_research
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/4

  Interface: Ten-GigabitEthernet1/0/2

  Direction: Outbound

  Policy: policy_market
   Classifier: classifier_market
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: behavior_market
      Mirroring:
        Mirror to the interface: Ten-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:
        Ten-GigabitEthernet1/0/10  Inbound
    Monitor egress port: Ten-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: Ten-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 Ten-GigabitEthernet1/0/4
traffic behavior behavior_market
 mirror-to interface Ten-GigabitEthernet1/0/4
#
qos policy policy_market
 classifier classifier_market behavior behavior_market
qos policy policy_research
 classifier classifier_research behavior behavior_research
#
interface Ten-GigabitEthernet1/0/1
 qos apply policy policy_research inbound
#
interface Ten-GigabitEthernet1/0/2
 qos apply policy policy_market outbound
#
interface Ten-GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 to 2
 mirroring-group 1 monitor-egress
#
interface Ten-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 Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
```

```
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
 mirroring-group 1 monitor-port
#
```

Example: Configuring granular traffic mirroring

Applicable product matrix

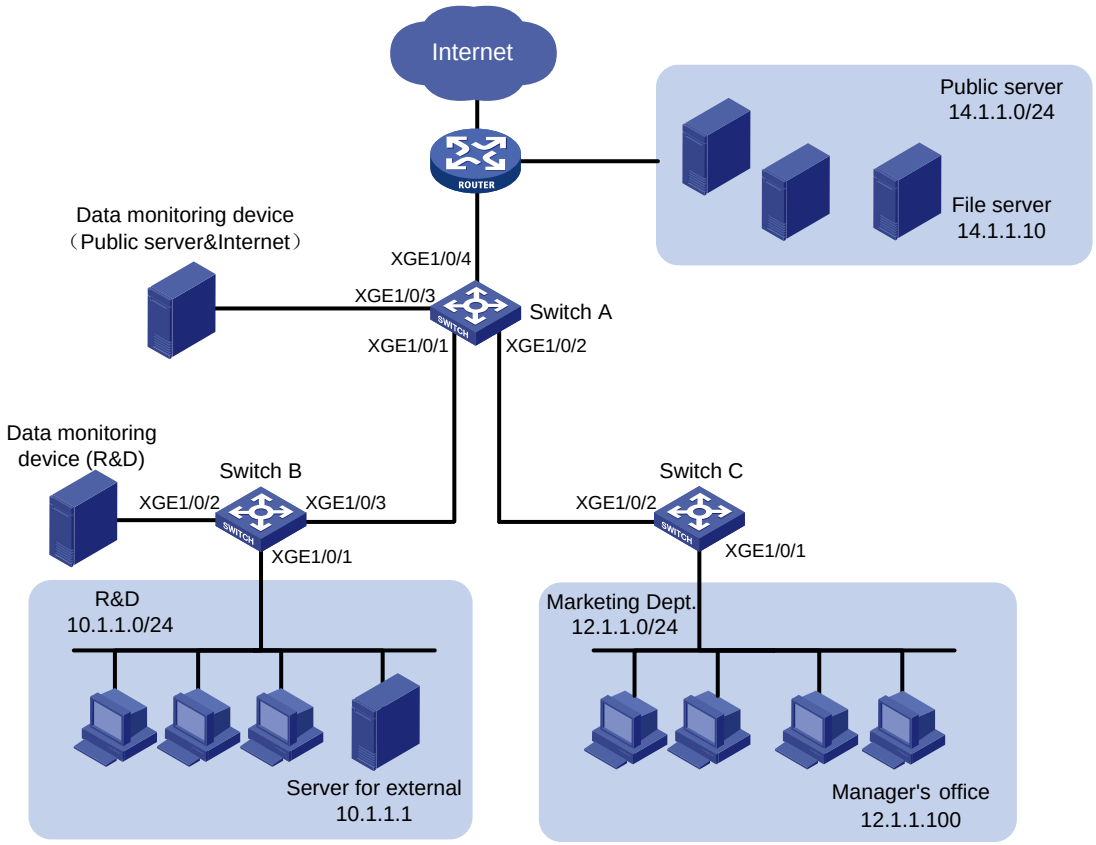
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 139, 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 during 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's office to the Internet.
- Monitor the traffic from the R&D Department only during non-working hours (18:00 to 8:30 of the next day) on working days.

Figure 139 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. Then issue this 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 Ten-GigabitEthernet 1/0/3.

```
[SwitchA] traffic behavior behavior_servers
[SwitchA-behavior-behavior_servers] mirror-to interface Ten-GigabitEthernet 1/0/3
[SwitchA-behavior-behavior_servers] quit
```

Create QoS policy **policy_servers**.

```
[SwitchA] qos policy policy_servers
```

Associate traffic class **classifier_servers** with traffic behavior **behavior_servers** in the QoS policy.

```
[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 Ten-GigabitEthernet 1/0/4.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] qos apply policy policy_servers inbound
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

2. Configure a QoS policy to filter packets from the file server during working hours:

Create a working-hour range named **work-time**, in which the working hours are from 8:30 to 18:00 on working days.

```
[SwitchA] time-range work-time 8:30 to 18:00 working-day
```

Create ACL 2001.

```
[SwitchA] acl number 2001
```

Configure a rule to permit packets from 14.1.1.10 during working hours on working days.

```
[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**.

```
[SwitchA] qos policy policy_fileserver
```

Associate traffic class **classifier_fileserver** with traffic behavior **behavior_fileserver** in the QoS policy.

```
[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 Ten-GigabitEthernet 1/0/3.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] qos apply policy policy_servers outbound
```

```
[SwitchA-Ten-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.

   ```
   [SwitchA] acl number 3000
   ```

   # Configure a rule to permit packets from subnet 12.1.1.0/24.

   ```
   [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 Ten-GigabitEthernet 1/0/3.

   ```
   [SwitchA] traffic behavior behavior_market
   [SwitchA-behavior-behavior_market] mirror-to interface Ten-GigabitEthernet 1/0/3
   [SwitchA-behavior-behavior_market] quit
   ```

2. Create a traffic class and a traffic behavior for the packets from the manager's office:

   # Create ACL 3001.

   ```
   [SwitchA] acl number 3001
   ```

   # Configure a rule to permit packets from 12.1.1.100.

   ```
   [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's office are issued first. The packets from the manager's office to access the Internet are not mirrored.

4. Apply QoS policy **policy_market** to the incoming packets of Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy policy_market inbound
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch B to mirror traffic from the R&D 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 source port Ten-GigabitEthernet 1/0/1.

```
[SwitchB] mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/1 inbound
```

   # Configure Ten-GigabitEthernet 1/0/2 as the monitor port of the mirroring group.

```
[SwitchB] mirroring-group 1 monitor-port Ten-GigabitEthernet 1/0/2
```

2. Configure an ACL to filter the outgoing traffic from the R&D Department during working hours:

   # Create a working-hour range named **work-time**, in which the working hours are from 8:30 to 18:00 on working days.

```
[SwitchB] time-range work-time 8:30 to 18:00 working-day
```

   # Create ACL 2000.

```
[SwitchB] acl number 2000
```

   # Configure a rule to permit packets from 10.1.1.1 during working hours on working days.

```
[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 Ten-GigabitEthernet 1/0/2.

```
[SwitchB] interface Ten-GigabitEthernet1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] packet-filter 2000 outbound
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface

Interface: Ten-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
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/3

Interface: Ten-GigabitEthernet1/0/3

  Direction: Outbound

  Policy: policy_servers
   Classifier: classifier_servers
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: behavior_servers
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/3

Interface: Ten-GigabitEthernet1/0/4

  Direction: Inbound

  Policy: policy_servers
   Classifier: classifier_servers
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: behavior_servers
      Mirroring:
        Mirror to the interface: Ten-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:
        Ten-GigabitEthernet1/0/1  Inbound
    Monitor port: Ten-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 Ten-GigabitEthernet1/0/3
traffic behavior behavior_fileserver
 filter deny
traffic behavior behavior_market
 mirror-to interface Ten-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 Ten-GigabitEthernet1/0/2
 qos apply policy policy_market inbound
#
interface Ten-GigabitEthernet1/0/3
 qos apply policy policy_servers outbound
#
```

```
interface Ten-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 Ten-GigabitEthernet1/0/1
 mirroring-group 1 mirroring-port inbound
#
interface Ten-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.

Example: Configuring IPv6 multicast group filters

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

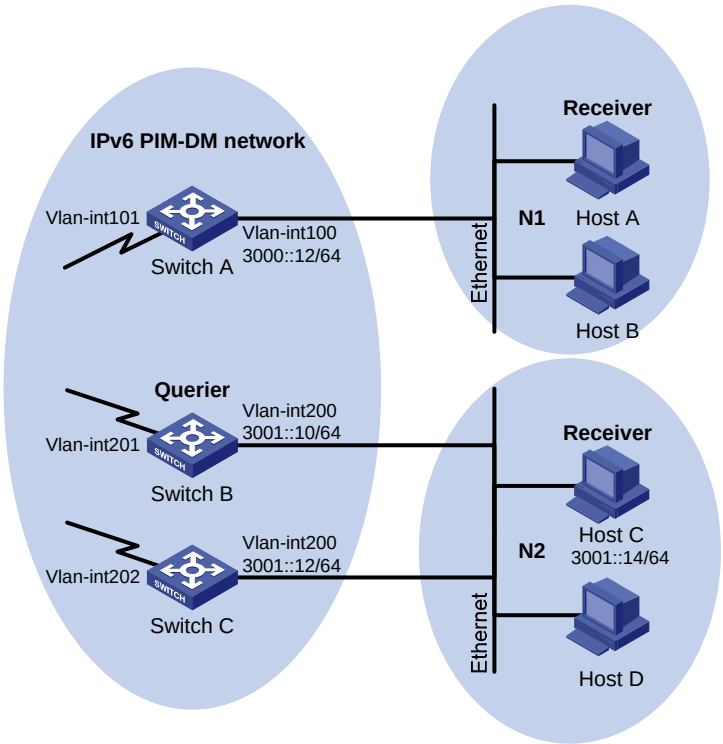
Network requirements

As shown in Figure 140:

- 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.
- All switches run OSPFv3, and they can communicate with each other through IPv6 unicast routes.

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 140 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Because multiple MLD-enabled switches exist in N2, you must configure the same IPv6 multicast group filter on these switches.
- To configure an IPv6 multicast group filter, you must create a basic IPv6 ACL, specifying the range of the IPv6 multicast groups that receiver hosts can join.

Configuration restrictions and guidelines

All Layer 3 switches on the same subnet must run the same version of MLD. Inconsistent versions of MLD on the Layer 3 switches on the same subnet might lead to inconsistency of MLD group membership.

Configuration procedures

1. Assign an IPv6 address to each interface of switches in the IPv6 PIM-DM domain, as shown in Figure 140. (Details not shown.)
2. Enable OSPFv3 on all switches on the IPv6 PIM-DM network. (Details not shown.)
3. Configure Switch A:

   # Enable IPv6 multicast routing globally.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6 multicast routing-enable
   ```

   # Enable MLD on VLAN-interface 100.

   ```
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] mld enable
   ```

   # Enable IPv6 PIM-DM on VLAN-interface 100 and VLAN-interface 101.

   ```
   [SwitchA-Vlan-interface100] ipv6 pim dm
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 101
   [SwitchA-Vlan-interface101] ipv6 pim dm
   [SwitchA-Vlan-interface101] quit
   ```

4. Configure Switch B:

   # Create an ACL rule, specifying the range of the IPv6 multicast groups that receiver hosts can join.

   ```
   <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] ipv6 multicast routing-enable
   ```

   # Enable MLD, and configure an IPv6 multicast group filter that references ACL 2001 on VLAN-interface 200.

   ```
   [SwitchB] interface vlan-interface 200
   [SwitchB-Vlan-interface200] mld group-policy 2001
   [SwitchB-Vlan-interface200] mld enable
   ```

   # Enable IPv6 PIM-DM on VLAN-interface 200.

```
[SwitchB-Vlan-interface200] ipv6 pim dm
[SwitchB-Vlan-interface200] quit
```

Enable IPv6 PIM-DM on VLAN-interface 201.

```
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] ipv6 pim dm
[SwitchB-Vlan-interface201] quit
```

5. Configure Switch C:

Create an ACL rule, specifying the range of the IPv6 multicast groups that receiver hosts can join.

```
<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] ipv6 multicast routing-enable
```

Enable MLD, and configure an IPv6 multicast group filter that references ACL 2001 on VLAN-interface 200.

```
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] mld group-policy 2001
```

Enable PIM-DM on VLAN-interface 200.

```
[SwitchC-Vlan-interface200] ipv6 pim dm
[SwitchC-Vlan-interface200] quit
```

Enable IPv6 PIM-DM on VLAN-interface 202.

```
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] ipv6 pim 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
 Vlan-interface200(FE80::223:89FF:FE5F:958B):
   MLD is enabled.
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Querier for MLD: FE80::223:89FF:FE5F:958B (this router)
  MLD groups reported in total: 1
```

Display information about the MLD querier on Switch C.

```
[SwitchC] display mld interface
 Vlan-interface200(FE80::223:89FF:FE5F:958C):
   MLD is enabled.
   MLD version: 1
   Query interval for MLD: 125s
```

```
    Other querier present time for MLD: 255s
    Maximum query response time for MLD: 10s
    Querier for MLD: FE80::223:89FF:FE5F:958B
  MLD groups reported in total: 1
```

The output shows that Switch B, with the smaller IPv6 link-local address, has become the MLD querier on this media-shared subnet.

2. Display information about MLD groups:

   # Send MLD reports from Host C in N2 to join IPv6 multicast groups **FF1E::101** and **FF1E::102**. (Details not shown.)

   # Display information about MLD groups on Switch B.

```
[SwitchB] display mld group
MLD groups in total: 1
 Vlan-interface200(FE80::223:89FF:FE5F:958B):
  MLD groups reported in total: 1
   Group address: FF1E::101
    Last reporter: FE80::10
    Uptime: 00:00:09
    Expires: 00:04:10
```

   # Display information about MLD groups on Switch C.

```
[SwitchC] display mld group
 MLD groups in total: 1
 Vlan-interface200(FE80::223:89FF:FE5F:958C):
  MLD groups reported in total: 1
   Group address: FF1E::101
    Last reporter: FE80::10
    Uptime: 00:00:10
    Expires: 00:03:13
```

   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 hosts in N2 can join only the IPv6 multicast group FF1E::101.

Configuration files

- Switch A:

```
#
 ipv6 multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 pim dm
 mld enable
#
interface Vlan-interface101
 ipv6 pim dm
#
```

- Switch B:

```
#
 ipv6 multicast routing-enable
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
vlan 200 to 201
#
interface Vlan-interface200
 ipv6 pim dm
 mld enable
 mld group-policy 2001
#
interface Vlan-interface201
 ipv6 pim dm
#
```

- Switch C:

```
#
 ipv6 multicast routing-enable
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
vlan 200
#
vlan 202
#
interface Vlan-interface200
 ipv6 pim dm
 mld enable
 mld group-policy 2001
 #
interface Vlan-interface202
 ipv6 pim dm
#
```

MLD snooping configuration examples

This chapter provides examples for configuring MLD snooping to manage and control IPv6 multicast group forwarding at Layer 2.

Example: Configuring an MLD snooping multicast group filter

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

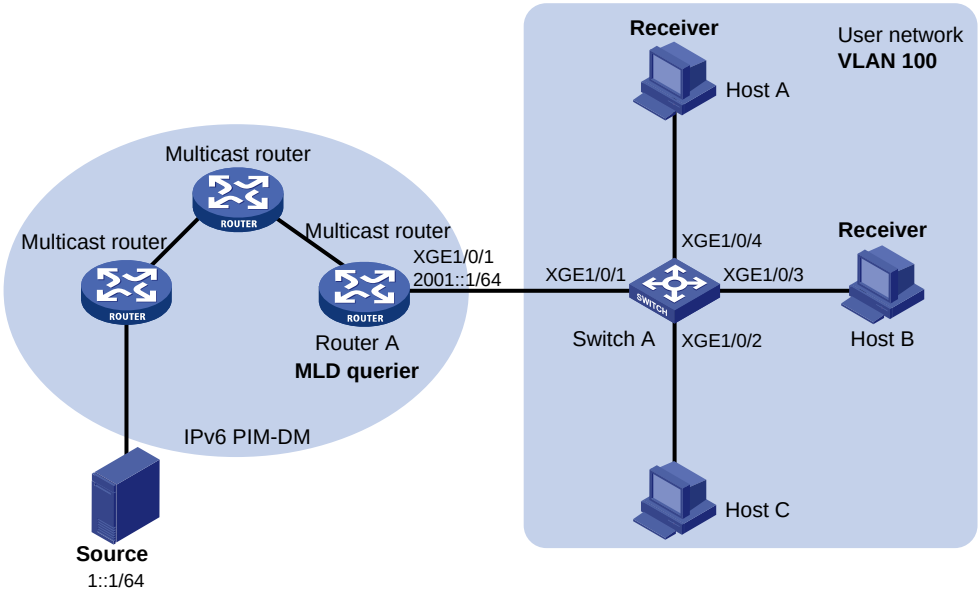
Network requirements

As shown in Figure 141:

- The 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 1::1/64.

Configure an MLD snooping multicast group filter on Switch A so the receiver hosts in VLAN 100 can receive only multicast packets destined for multicast group FF1E::101.

Figure 141 Network diagram



Requirements analysis

To prevent the receiver hosts in VLAN 100 from receiving multicast packets for other IPv6 multicast groups, enable dropping unknown IPv6 multicast packets for VLAN 100.

To configure an IPv6 multicast group filter, create a basic IPv6 ACL, specifying the range of IPv6 multicast groups that receiver hosts can join.

Configuration restrictions and guidelines

If the IPv6 ACL specified for the MLD snooping multicast group filter does not exist or it has no rule, the filter will filter out all multicast groups.

Configuration procedures

Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port ten-gigabitethernet 1/0/1 to ten-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
```

Create an IPv6 ACL, specifying the range of IPv6 multicast groups that receiver hosts can join.

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
```

Configure an IPv6 multicast group filter that references IPv6 ACL 2001 for VLAN 100.

```
[SwitchA] mld-snooping
[SwitchA-mld-snooping] group-policy 2001 vlan 100
[SwitchA-mld-snooping] quit
```

Verifying the configuration

Send MLD reports from Host A and Host B to join the IPv6 multicast groups **FF1E::101** and **FF1E::102**, respectively. (Details not shown.)

Display MLD snooping forwarding entry information of dynamic IPv6 multicast groups for VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (1 in total):
      XGE1/0/4         (00:03:15)
```

The output shows that Switch A has only the entry for IPv6 multicast group FF1E::101. The filter is functioning.

Configuration files

```
#
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 Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Configuring MLD snooping static ports

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

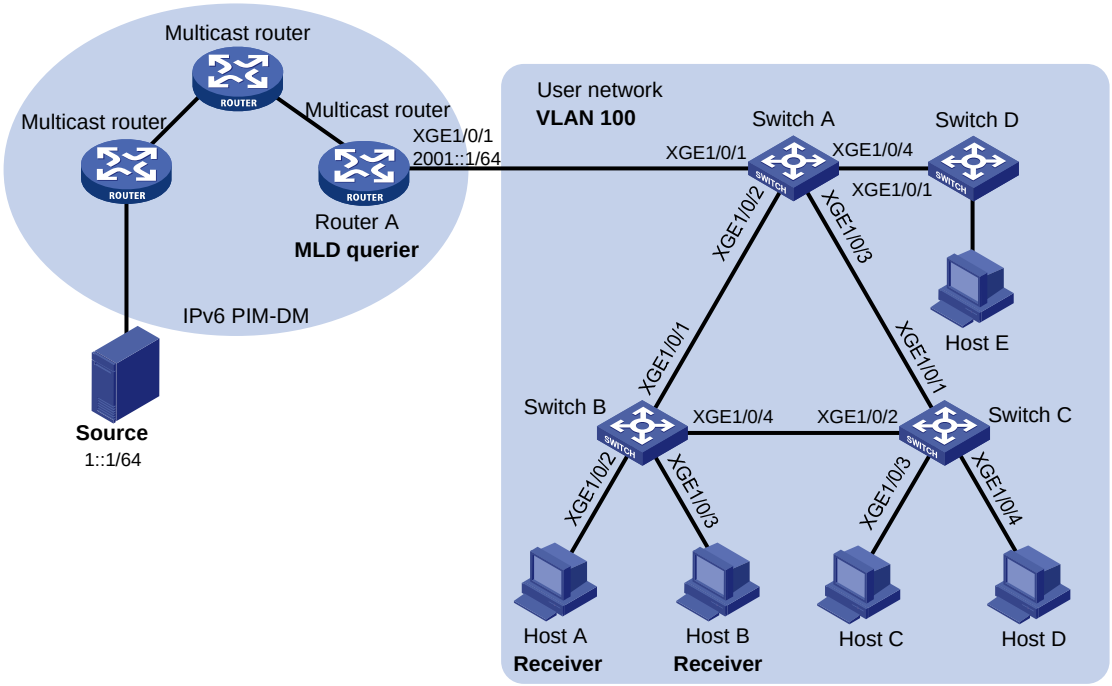
As shown in Figure 142:

- The 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.
- In the user network, dropping unknown IPv6 multicast packets is enabled on all switches to prevent unknown IPv6 multicast packets from being flooded.

Configure MLD snooping static member ports and MLD snooping static router ports to achieve the following goals:

- Host A and Host B receive only multicast packets destined for the 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 142 Network diagram



Requirements analysis

To enable the receiver hosts to receive multicast packets for a fixed IPv6 multicast group, configure the ports on the switches that are connected to the hosts as MLD snooping static member ports of the IPv6 multicast group.

After an STP switchover 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. To implement the immediate switchover to the new path, you must configure all ports that might become multicast packet outbound ports as MLD snooping static router ports.

Configuration procedures

Configuring Switch A

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
```

Enable MLD snooping for VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 as MLD snooping static router ports.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchA-Ten-GigabitEthernet1/0/2] quit
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configuring Switch B

Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/4
```

Enable MLD snooping for VLAN 100.

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 as MLD snooping static member ports of the IPv6 multicast group **FF1E::101**.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-Ten-GigabitEthernet1/0/2] quit
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configuring Switch C

Enable MLD snooping globally.

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
```

Enable MLD snooping for VLAN 100.

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/2 as an MLD snooping static router port.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about MLD snooping static router ports for VLAN 100 on Switch A and Switch C.

```
[SwitchA] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/2
    XGE1/0/3
[SwitchC] display mld-snooping static-router-port vlan 100
VLAN 1:
  Router slots (0 in total):
  Router ports (1 in total):
    XGE1/0/2
```

The output shows that Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 on Switch A and Ten-GigabitEthernet 1/0/2 on Switch C are MLD snooping static router ports.

Display information about MLD snooping forwarding entries of static IPv6 multicast groups for VLAN 100 on Switch B.

```
[SwitchB] display mld-snooping static-group vlan 100
Total 1 entries.

VLAN 1: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (2 in total):
      XGE1/0/2
      XGE1/0/3
```

The output shows that Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 on Switch B are MLD snooping static member ports for the IPv6 multicast forwarding entry (::, FF1E::101).

Configuration files

- Switch A:

```
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch B:

```
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 mld-snooping static-group ff1e::101 vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping static-group ff1e::101 vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

- Switch C:

```
#
 mld-snooping
```

```
#
vlan 100
 mld-snooping enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

NQA configuration examples

This chapter provides NQA configuration examples.

Example: Configuring an ICMP echo operation

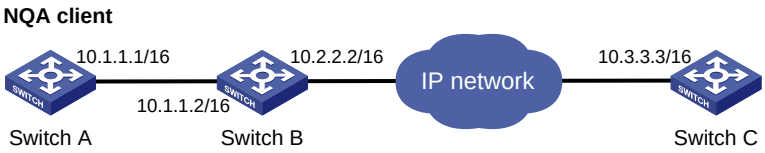
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 143, 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 143 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 after the operation is 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: 2013-09-25 14:08:29.7
    Extend results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 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
    280        2            Succeeded        2013-09-25 14:10:04.7
    279        2            Succeeded        2013-09-25 14:10:04.7
    278        2            Succeeded        2013-09-25 14:10:04.7
    277        2            Succeeded        2013-09-25 14:10:04.7
    276        2            Succeeded        2013-09-25 14:10:04.7
    275        2            Succeeded        2013-09-25 14:10:04.7
    274        2            Succeeded        2013-09-25 14:10:04.7
    273        2            Succeeded        2013-09-25 14:10:04.7
    272        2            Succeeded        2013-09-25 14:10:04.7
    271        2            Succeeded        2013-09-25 14:10:04.7
```

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 UDP echo operation

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 144, configure a UDP echo operation to test the round-trip time between Switch A and Switch B.

Figure 144 Network diagram

Configurations restrictions and guidelines

When you configure an NQA 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 after the operation is finished.

Configuration procedures

Configuring Switch B

Enable the NQA server, and configure a listening service to listen to the IP address 10.2.2.2 and UDP port 8000.

```
<SwitchB> system-view
[SwitchB] nqa server enable
[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: 10/10/10
      Square-Sum of round trip time: 100
      Last succeeded probe time: 2013-09-25 14:20:32.6
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 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          10           Succeeded        2013-09-25 14:20:32.6
```

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
#
```

NTP configuration examples

This chapter provides NTP configuration examples.

Table 16 NTP association modes

Mode	Clock source	Time accuracy	Guidelines
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 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	If the stratum in the first broadcast message that a client receives from a server is lower than the stratum of the client, the client does the following: • Uses the server as the clock source. • 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	Guidelines
Multicast	If the stratum in the first multicast message that a client receives from a server is lower than the stratum of the client, the client does the following: • Uses the server as the clock source. • 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.

Configuration restrictions and guidelines

Example: Configuring the NTP client/server mode

Applicable product matrix

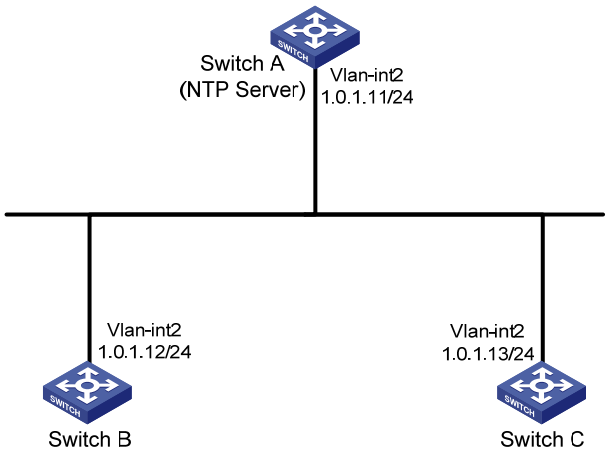
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 145, 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 145 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2 on Switch A.

   ```
   [SwitchA] ntp-service refclock-master 2
   ```

2. Configure Switch B:

   # Enable the NTP service.

   ```
   <SwitchB> system-view
   [SwitchB] ntp-service enable
   ```

   # Specify Switch A as the NTP server of Switch B.

   ```
   [SwitchB] ntp-service unicast-server 1.0.1.11
   ```

3. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify Switch A as the NTP server of Switch C:

   ```
   [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
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
```

```
 Leap indicator: 00
 Clock jitter: 0.003479 s
 Stability: 0.000 pps
 Clock precision: 2^-15
 Root delay: 1.95313 ms
 Root dispersion: 28.38135 ms
 Reference time: d5ed8cd5.577006ea  Wed, Sep 25 2013 16:24:53.341
```

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   255   64   38 -10.22 1.9531 3.3416
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

The output shows that an association has been established between Switch B and Switch A.

Configuration files

- Switch A:

```
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Switch B:

```
#
 ntp-service enable
 ntp-service unicast-server 1.0.1.11
#
```

- Switch C:

```
#
 ntp-service enable
 ntp-service unicast-server 1.0.1.11
#
```

Example: Configuring the IPv6 NTP client/server mode

Applicable product matrix

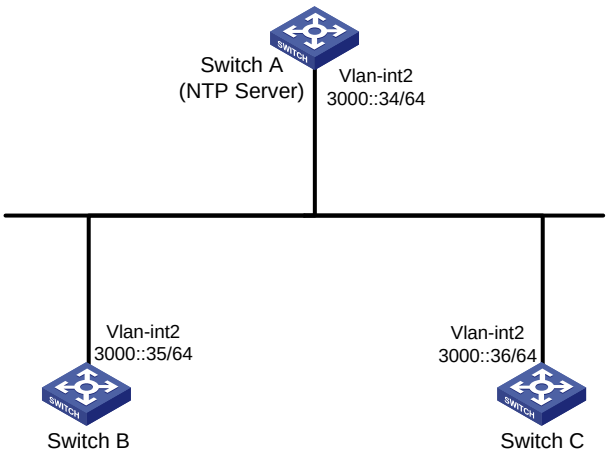
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 146, 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 146 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

   ```
   [SwitchA] ntp-service refclock-master 2
   ```

2. Configure Switch B:

   # Enable the NTP service.

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

```
[SwitchB] ntp-service enable
```

Specify Switch A as the NTP server of Switch B.

```
[SwitchB] ntp-service ipv6 unicast-server 3000::34
```

3. Configure Switch C:

Enable the NTP service.

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

Specify Switch A as the NTP server of Switch C:

```
[SwitchC] ntp-service ipv6 unicast-server 3000::34
```

Verifying the configuration

Display the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3000::34
 Local mode: client
 Reference clock ID: 95.197.17.40
 Leap indicator: 00
 Clock jitter: 0.000046 s
 Stability: 0.000 pps
 Clock precision: 2^-15
 Root delay: 1.81580 ms
 Root dispersion: 387.78687 ms
 Reference time: d5f3c993.117a884a  Mon, Sep 30 2013  9:57:39.068
```

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 ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source: [12345]3000::34
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 3               Poll interval: 64
 Last receive time: 62           Offset: 0.1272
 Roundtrip delay: 1.8158         Dispersion: 188.47

 Total sessions: 1
```

The output shows that an association has been established between Switch B and Switch A.

Configuration files

- Switch A:

```
#
 ntp-service enable
```

```
 ntp-service refclock-master 2
#
```

- Switch B:

```
#
 ntp-service enable
 ntp-service ipv6 unicast-server 3000::34
#
```

- Switch C:

```
#
 ntp-service enable
 ntp-service ipv6 unicast-server 3000::34
#
```

Example: Configuring the NTP symmetric active/passive mode

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

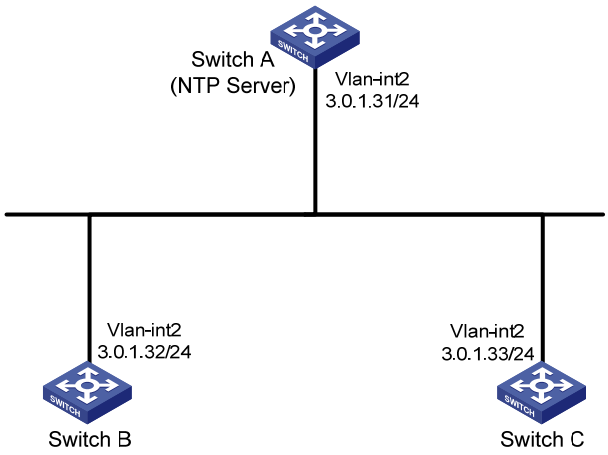
Network requirements

As shown in Figure 147, 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 147 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

   ```
   [SwitchA] ntp-service refclock-master 2
   ```

2. Configure Switch B:

   # Enable the NTP service.

   ```
   <SwitchB> system-view
   [SwitchB] ntp-service enable
   ```

   # Specify Switch A as the NTP server of Switch B.

   ```
   [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
    System peer: 3.0.1.31
    Local mode: client
    Reference clock ID: 3.0.1.31
    Leap indicator: 00
    Clock jitter: 0.003479 s
    Stability: 0.000 pps
    Clock precision: 2^-15
    Root delay: 1.95313 ms
    Root dispersion: 28.38135 ms
    Reference time: d5ed8cd5.577006ea  Wed, Sep 25 2013 16:50:56.521
   ```

   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.

3. Configure Switch C:

Enable the NTP service.

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

Specify Switch A as the NTP server of Switch C.

```
[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
 System peer: 3.0.1.32
 Local mode: sym_active
 Reference clock ID: 3.0.1.32
 Leap indicator: 00
 Clock jitter: 0.000031 s
 Stability: 0.000 pps
 Clock precision: 2^-15
 Root delay: 1.89209 ms
 Root dispersion: 7976.83716 ms
 Reference time: d5ed991e.577a410f  Wed, Sep 25 2013 16:52:28.341
```

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 enable
 ntp-service refclock-master 2
#
```

- Switch B:

```
#
 ntp-service enable
 ntp-service unicast-server 3.0.1.31
#
```

- Switch C:

```
#
 ntp-service enable
 ntp-service unicast-server 3.0.1.31
 ntp-service unicast-peer 3.0.1.32
#
```

Example: Configuring the IPv6 NTP symmetric active/passive mode

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

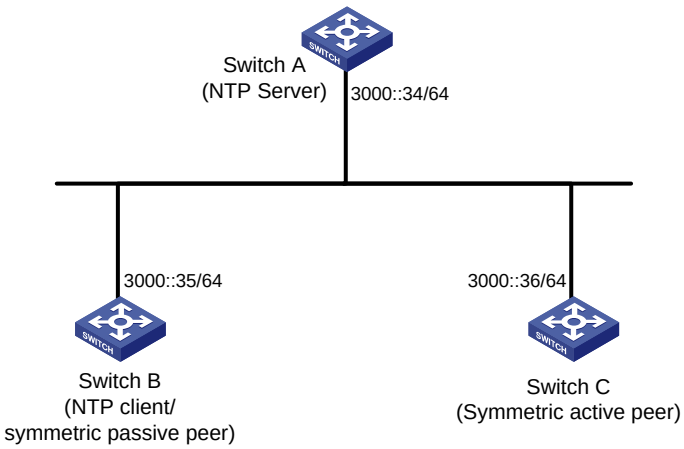
Network requirements

As shown in Figure 148, 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 148 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

   ```
   [SwitchA] ntp-service refclock-master 2
   ```

2. Configure Switch B:

   # Enable the NTP service.

```
<SwitchB> system-view
[SwitchB] ntp-service enable
```

Specify Switch A as the NTP server of Switch B.

```
[SwitchB] ntp-service ipv6 unicast-server 3000::34
```

Display the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3000::34
 Local mode: client
 Reference clock ID: 95.197.17.40
 Leap indicator: 00
 Clock jitter: 0.000031 s
 Stability: 0.000 pps
 Clock precision: 2^-15
 Root delay: 1.90735 ms
 Root dispersion: 15.57922 ms
 Reference time: d5f403b3.1179ffb4  Mon, Sep 30 2013 14:05:39.068
```

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.

3. Configure Switch C:

Enable the NTP service.

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 3.

```
[SwitchC] ntp-service refclock-master 3
```

Specify Switch A as the NTP server of Switch C.

```
[SwitchC] ntp-service ipv6 unicast-server 3000::34
```

Configure Switch B as a symmetric passive peer of Switch C.

```
[SwitchC] ntp-service ipv6 unicast-peer 3000::35
```

Verifying the configuration

Disconnect Switch A from the network. Display the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 System peer: 3000::36
 Local mode: sym_active
 Reference clock ID: 251.73.79.32
 Leap indicator: 00
 Clock jitter: 0.000549 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 4.21143 ms
 Root dispersion: 19.80591 ms
```

```
Reference time: d5f4053f.bf8775ef  Mon, Sep 30 2013 14:12:15.748
```

The output shows that Switch B has synchronized to Switch C. The clock stratum level is 4 on Switch B and 3 on Switch C.

Configuration files

- Switch A:

```
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Switch B:

```
#
 ntp-service enable
 ntp-service ipv6 unicast-server 3000::34
#
```

- Switch C:

```
#
 ntp-service enable
 ntp-service refclock-master 3
 ntp-service ipv6 unicast-server 3000::34
 ntp-service ipv6 unicast-peer 3000::35
#
```

Example: Configuring the NTP broadcast mode

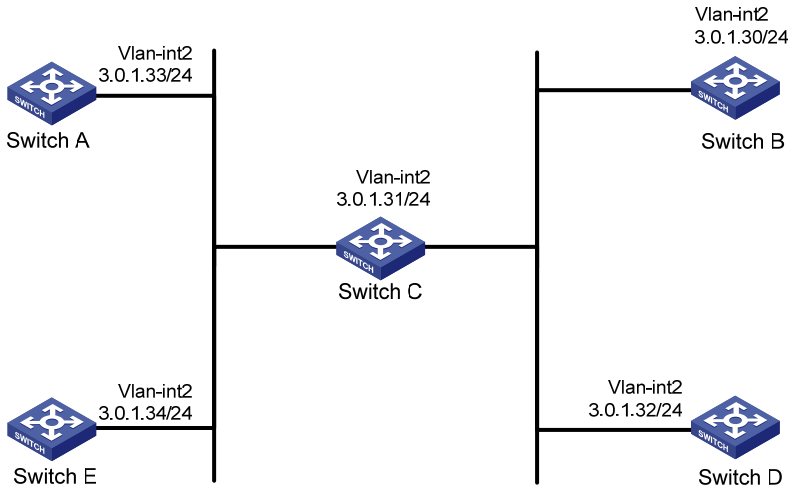
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 149, configure NTP to synchronize the time among multiple devices on a subnet.

Figure 149 Network diagram



Configuration procedures

1. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2 on Switch C.

   ```
   [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
   ```

2. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Configure Switch A to operate in broadcast client mode and receive 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 the NTP status of Switch A after clock synchronization.

```
[SwitchA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
```

```
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000061 s
 Stability: 0.000 pps
 Clock precision: 2^-14
 Root delay: 0.00000 ms
 Root dispersion: 7951.43127 ms
 Reference time: d5ee8d88.2faabed0  Thu, Sep 26 2013 10:40:08.186
```

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   82 -2.190 0.0000 7937.5
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

The output shows that an association has been established between Switch A and Switch C.

Configuration files

- Switch C:

```
#
 ntp-service enable
 ntp-service refclock-master 2
#
interface Vlan-interface2
 ntp-service broadcast-server
#
```

- Switch A:

```
#
 ntp-service enable
interface Vlan-interface2
 ntp-service broadcast-client
#
```

- Switch B:

```
#
 ntp-service enable
interface Vlan-interface2
 ntp-service broadcast-client
#
```

- Switch D:

```
#
 ntp-service enable
interface Vlan-interface2
```

```
 ntp-service broadcast-client
#
```

- Switch E:

```
#
 ntp-service enable
interface Vlan-interface2
 ntp-service broadcast-client
#
```

Example: Configuring the NTP multicast mode

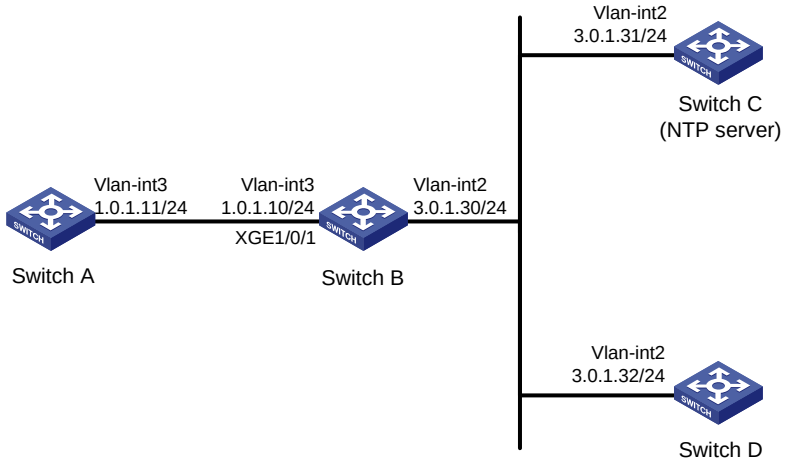
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 150, configure NTP to synchronize the time among multiple devices on different subnets.

Figure 150 Network diagram



Configuration procedures

1. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

```
[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
```

2. Configure Switch D:

Enable the NTP service.

```
<SwitchD> system-view
[SwitchD] ntp-service enable
```

Configure Switch D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

3. Configure Switch B:

Enable the NTP service.

```
<SwitchB> system-view
[SwitchB] ntp-service enable
```

Configure Switch B to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ntp-service multicast-client
[SwitchB-Vlan-interface2] quit
```

Configure multicast functions on Switch B.

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim dm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port Ten-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] igmp-snooping
[SwitchB-igmp-snooping] quit
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

4. Configure Switch A:

Enable the NTP service.

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

Configure Switch A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
[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
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000061 s
 Stability: 0.000 pps
 Clock precision: 2^-14
 Root delay: 1.69373 ms
 Root dispersion: 1950.18005 ms
 Reference time: d5ee9b15.2f3a684d  Thu, Sep 26 2013 11:37:57.184
```

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 enable
#
interface Vlan-interface3
 ntp-service multicast-client
#
```

- Switch B:

```
#
ntp-service enable
#
multicast routing-enable
#
igmp-snooping
#
interface Vlan-interface2
 pim dm
 ntp-service multicast-client
#
interface Vlan-interface3
 igmp enable
 igmp static-group 224.0.1.1
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 3
 igmp-snooping static-group 224.0.1.1 vlan 3
```

```
#
```

- Switch C:

```
#
 ntp-service enable
ntp-service refclock-master 2
#
interface Vlan-interface2
 ntp-service multicast-server
#
```

- Switch D:

```
#
 ntp-service enable
#
interface Vlan-interface2
 ntp-service multicast-client
#
```

Example: Configuring the IPv6 NTP multicast mode

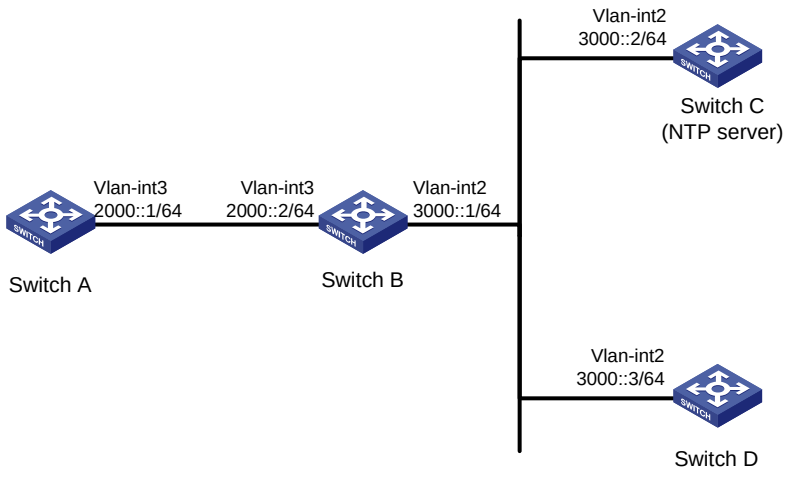
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 151, configure NTP to synchronize the time among multiple devices on different subnets.

Figure 151 Network diagram



Configuration procedures

1. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

   ```
   [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 ipv6 multicast-server ff24::1
   ```

2. Configure Switch D:

   # Enable the NTP service.

   ```
   <SwitchD> system-view
   [SwitchD] ntp-service enable
   ```

   # Configure Switch D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

   ```
   [SwitchD] interface vlan-interface 2
   [SwitchD-Vlan-interface2] ntp-service ipv6 multicast-client ff24::1
   ```

3. Configure Switch B:

   # Enable the NTP service.

   ```
   <SwitchB> system-view
   [SwitchB] ntp-service enable
   ```

   # Configure Switch B to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

   ```
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ntp-service ipv6 multicast-client ff24::1
   [SwitchB-Vlan-interface2] quit
   ```

   # Configure multicast functions on Switch B.

   ```
   [SwitchB] ipv6 multicast routing-enable
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ipv6 pim dm
   [SwitchB-Vlan-interface2] quit
   [SwitchB] vlan 3
   [SwitchB-vlan3] port Ten-GigabitEthernet 1/0/1
   [SwitchB-vlan3] quit
   [SwitchB] interface vlan-interface 3
   [SwitchB-Vlan-interface3] mld enable
   [SwitchB-Vlan-interface3] mld static-group ff24::1
   [SwitchB-Vlan-interface3] quit
   [SwitchB] mld-snooping
   [SwitchB-mld-snooping] quit
   [SwitchB] interface Ten-GigabitEthernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] mld-snooping static-group ff24::1 vlan 3
   ```

4. Configure Switch A:

Enable the NTP service.

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

Configure Switch A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service ipv6 multicast-client ff24::1
```

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
 System peer: 3000::2
 Local mode: bclient
 Reference clock ID: 165.84.121.65
 Leap indicator: 00
 Clock jitter: 0.165741 s
 Stability: 0.000 pps
 Clock precision: 2^-10
 Root delay: 0.00534 ms
 Root dispersion: 4.51282 ms
 Reference time: d0c61289.10b1193f  Mon, Sep 30 2013 18:32:15.748
```

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 enable
#
interface Vlan-interface3
 ntp-service ipv6 multicast-client ff24::1
#
```

- Switch B:

```
#
ntp-service enable
#
ipv6 multicast routing-enable
#
mld-snooping
#
interface Vlan-interface2
 ipv6 pim dm
 ntp-service ipv6 multicast-client ff24::1
```

```
#
interface Vlan-interface3
 mld enable
 mld static-group ff24::1
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 3
 mld-snooping static-group ff24::1 vlan 3
#
```

- Switch C:

```
#
 ntp-service enable
ntp-service refclock-master 2
#
interface Vlan-interface2
 ntp-service ipv6 multicast-server ff24::1
#
```

- Switch D:

```
#
 ntp-service enable
#
interface Vlan-interface2
 ntp-service ipv6 multicast-client ff24::1
#
```

Example: Configuring the NTP client/server mode with authentication

Applicable product matrix

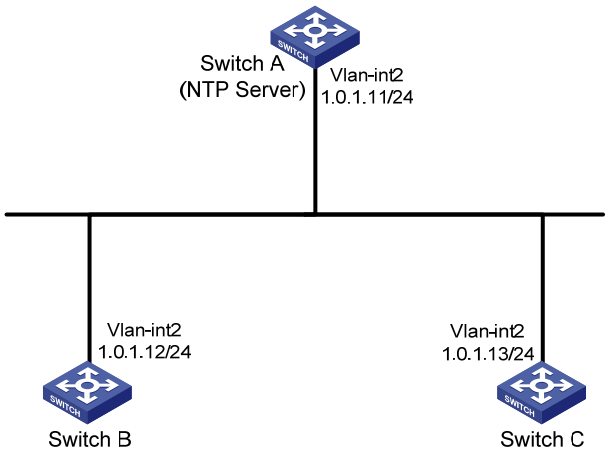
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

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 operates in client mode, and Switch A is the NTP server for Switch B.
- Configure NTP authentication on both Switch A and Switch B.

Figure 152 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

   ```
   [SwitchA] ntp-service refclock-master 2
   ```

   # Enable NTP authentication on Switch A.

   ```
   [SwitchA] ntp-service authentication enable
   ```

   # Configure an NTP authentication key, with the key ID of **42** and key value of **aNiceKey**. Input the key in plain text.

   ```
   [SwitchA] ntp-service authentication-keyid 42 authentication-mode md5 simple
   aNiceKey
   ```

   # Specify the key as a trusted key.

   ```
   [SwitchA] ntp-service reliable authentication-keyid 42
   ```

2. Configure Switch B:

   # Enable the NTP service.

   ```
   <SwitchB> system-view
   [SwitchB] ntp-service enable
   ```

   # Enable NTP authentication on Switch B.

   ```
   [SwitchB] ntp-service authentication enable
   ```

   # Configure an NTP authentication key, with the key ID of **42** and key value of **aNiceKey**. Input the key in plain text.

   ```
   [SwitchB] ntp-service authentication-keyid 42 authentication-mode md5 simple
   aNiceKey
   ```

   # Specify the key as a trusted key.

   ```
   [SwitchB] ntp-service reliable authentication-keyid 42
   ```

   # Specify Switch A as the NTP server of Switch B, and associate the server with key 42.

   ```
   [SwitchB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
   ```

3. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Enable NTP authentication on Switch C.

   ```
   [SwitchC] ntp-service authentication enable
   ```

   # Configure an NTP authentication key, with the key ID of **42** and key value of **aNiceKey**. Input the key in plain text.

   ```
   [SwitchC] ntp-service authentication-keyid 42 authentication-mode md5 simple
   aNiceKey
   ```

   # Specify the key as a trusted key.

   ```
   [SwitchC] ntp-service reliable authentication-keyid 42
   ```

   # Specify Switch A as the NTP server of Switch C, and associate the server with key 42.

   ```
   [SwitchC] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
   ```

Verifying the configuration

Display NTP service status on Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-10
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Mon, Sep 30 2013 16:06:26.764
```

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 IPv4 NTP association information for Switch B.

```
[SwitchB] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]1.0.1.11        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions : 1
```

The output shows that an association has been established between Switch B and Switch A.

Configuration files

- Switch A:

  ```
  #
  ```

```
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$4j3SKCgQWBK3Un41B9U0JXzJX9i7IuNoSqi
 ntp-service reliable authentication-keyid 42
 ntp-service refclock-master 2
#
```

- Switch B:

```
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$22eIc8l796cpudZqiaAZ2SLzIfrgzFTVYn8X
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 1.0.1.11 authentication-keyid 42
#
```

- Switch C:

```
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$XJzVmJ1TJbWyYAXpPXxF7JiEOZag8CehibM8
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 1.0.1.11 authentication-keyid 42
#
```

Example: Configuring the NTP broadcast mode with authentication

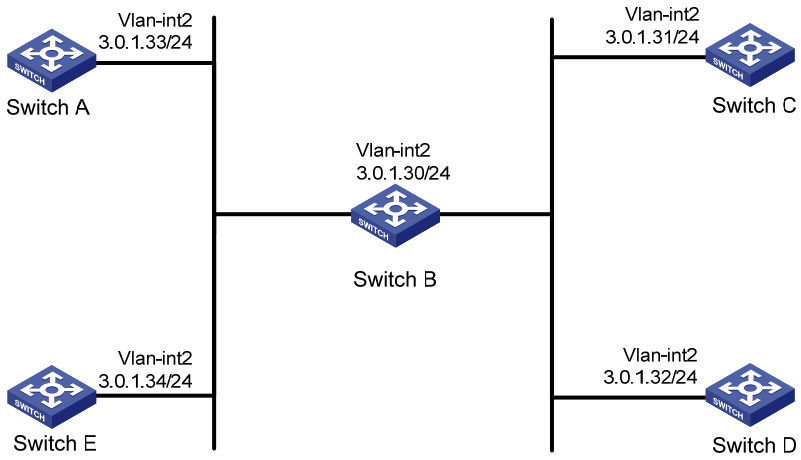
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 153, configure NTP to synchronize the time among multiple devices on a subnet. Configure NTP authentication to prevent attacks.

Figure 153 Network diagram



Configuration procedures

1. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2 on Switch C.

   ```
   [SwitchC] ntp-service refclock-master 2
   ```

   # Enable NTP authentication on Switch C. Configure an NTP authentication key, with the key ID of **88** and key value of **123456**. Input the key in plain text, and specify it as a trusted key.

   ```
   [SwitchC] ntp-service authentication enable
   [SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
   [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 the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Enable NTP authentication on Switch A. Configure an NTP authentication key, with the key ID of **88** and key value of **123456**. Input the key in plain text, and specify it as a trusted key.

   ```
   [SwitchA] ntp-service authentication enable
   [SwitchA] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
   [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
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000092 s
 Stability: 0.000 pps
 Clock precision: 2^-14
 Root delay: 2.42615 ms
 Root dispersion: 1950.98877 ms
 Reference time: d5eed631.2f498d71  Thu, Sep 26 2013 15:50:09.184
```

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 enable
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5 cipher
$c$3$iJudDKiqCVO+gOaG5363/fz4M3dQvHo2Fw==
 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 enable
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5 cipher
$c$3$pU6KvpS80MadhM2zMCCSR07HX4qEbJhHvQ==
 ntp-service reliable authentication-keyid 88
#
```

Example: Configuring SNTP

Applicable product matrix

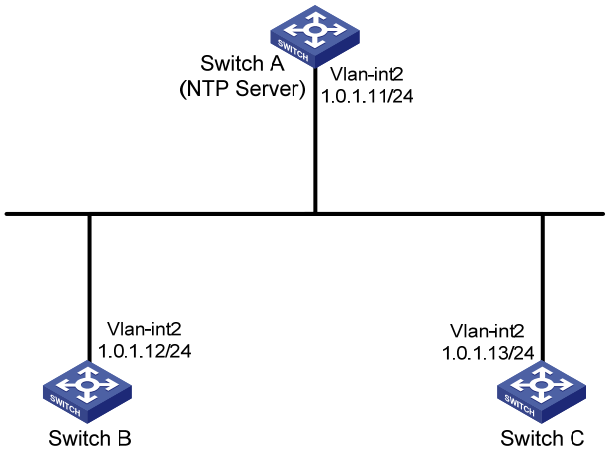
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 154, configure SNTP 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 SNTP client mode.
- Switch A is the NTP server for Switch B and Switch C.

Figure 154 Network diagram



Configuration procedures

1. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with the stratum level 2.

   ```
   [SwitchA] ntp-service refclock-master 2
   ```

2. Configure Switch B:

   # Enable the SNTP service.

   ```
   <SwitchB> system-view
   [SwitchB] sntp enable
   ```

   # Specify Switch A as the NTP server of Switch B.

```
[SwitchB] sntp unicast-server 1.0.1.11
```

3. Configure Switch C:

   # Enable the SNTP service.

```
<SwitchC> system-view
[SwitchC] sntp enable
```

   # Specify Switch A as the NTP server of Switch C.

```
[SwitchC] sntp unicast-server 1.0.1.11
```

Verifying the configuration

Display SNTP association information for Switch B after clock synchronization.

```
[SwitchB] display sntp sessions
SNTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Thu, Sep 26 2013 17:25:09.121 (Synced)
```

The output shows that an association has been established between Switch B and Switch A.

Configuration files

- Switch A:

```
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Switch B:

```
#
 sntp enable
 sntp unicast-server 1.0.1.11
#
```

- Switch C:

```
#
 sntp enable
 sntp unicast-server 1.0.1.11
#
```

OSPF configuration examples

This chapter provides OSPF configuration examples.

Example: Configuring basic OSPF

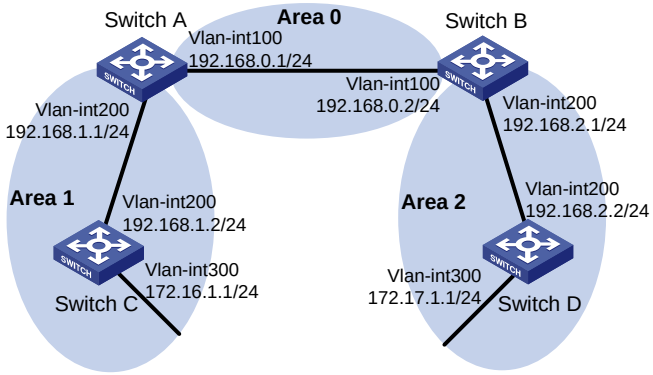
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 155, configure OSPF on the switches, and split the AS into three OSPF areas.

Figure 155 Network diagram



Configuration restrictions and guidelines

OSPF uses a router ID to identify a switch. Make sure any two switches in an AS have different router IDs.

Configuration procedures

1. Configure IP addresses for the interfaces, as shown in Figure 155. (Details not shown.)
2. Enable OSPF:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf 1 router-id 192.168.1.1
[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] ospf 1 router-id 192.168.2.1
[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] ospf 1 router-id 192.168.1.2
[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] ospf 1 router-id 192.168.2.2
[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 OSPF GR

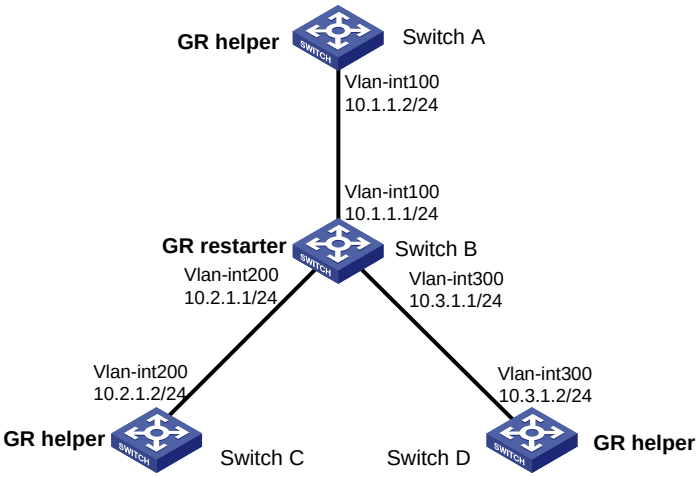
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 156, configure IETF Graceful Restart (GR) on Switch B. This avoids route flapping, route changes, or forwarding interruption during an active/standby switchover or a routing protocol restart.

Figure 156 Network diagram



Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 156. (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 Switch B as the IETF OSPF GR restarter.

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] graceful-restart ietf
```

Verifying the configuration

Restart the OSPF process on Switch B to trigger GR. During the GR process, verify that:

- The routing tables of the switches do not have any changes.
- Network interruption does not occur (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
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
 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
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
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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 157:

- Run OSPF on Switch A, Switch B, and Switch C so that they can reach each other at the network layer.
- Configure OSPF BFD on Switch A and Switch B.

  When the link over which Switch A and Switch B communicate through a Layer 2 switch fails, the switches can quickly detect the failure and notify OSPF of the failure. Switch A and Switch B then communicate through Switch C.

Figure 157 Network diagram

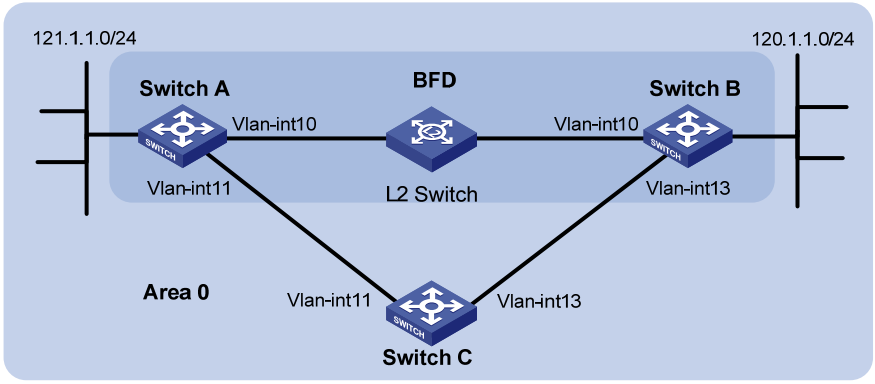


Table 17 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int10	10.1.0.102/24	Switch B	Vlan-int13	13.1.1.1/24
Switch A	Vlan-int11	11.1.1.1/24	Switch C	Vlan-int11	11.1.1.2/24
Switch B	Vlan-int10	10.1.0.100/24	Switch C	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 157. (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
#
```

Password control configuration examples

This chapter provides password control configuration examples.

General restrictions and guidelines

When you configure password control, follow these restrictions and guidelines:

- In FIPS mode, the password control feature is enabled by default, and it cannot be disabled.
- To successfully enable the global password control feature and allow device management users to log in to the device, the device must have sufficient storage space.

Example: Configuring password control

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

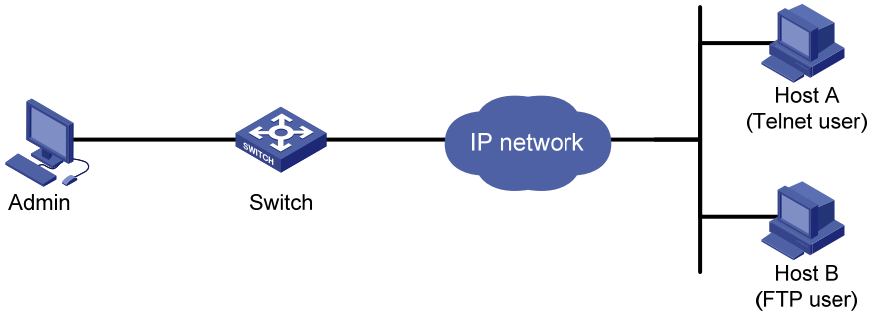
Network requirements

As shown in Figure 158:

- Configure a global password control policy to meet the following requirements:
  - A user failing to provide the correct password in two successive login attempts is permanently prohibited from logging in.
  - A user can log in five times within 60 days after the password expires.
  - A password expires after 30 days.
  - The minimum password update interval is 36 hours.
  - The maximum account idle time is 30 days.
  - A password cannot contain the username or the reverse of the username.
  - No character appears consecutively three or more times in a password.
- Configure the local Telnet user **telnet-user** with a password control policy for user role **level-0** to meet the following requirements:
  - The password must contain at least 20 characters.
  - The password must contain four character types and at least four characters for each type.
- Configure the local FTP user **ftp-user** with a password control policy for user role **level-9** to meet the following requirements:
  - The password must contain at least 24 characters.
  - The password must contain four character types and at least five characters for each type.

- The password for the local user expires after one day.

Figure 158 Network diagram



Configuration restrictions and guidelines

When you configure password control, follow these restrictions and guidelines:

- When passwords expire, Telnet users, SSH users, and console users can change their own passwords, but FTP users cannot. Only the administrator can change passwords for FTP users.
- After the global password control feature is enabled, you cannot display the password configuration for local device management users by using the corresponding **display** commands.

Configuration procedures

Enable the Telnet server function.

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

Enable the FTP server function.

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

Configure authentication mode as AAA and Telnet protocol as **all** for VTP user interfaces.

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

Enable the password control feature globally.

```
[Switch] password-control enable
```

Prohibit the user from logging in forever after two successive login failures.

```
[Switch] password-control login-attempt 2 exceed lock
```

Set all passwords to expire after 30 days.

```
[Switch] password-control aging 30
```

Set the minimum password update interval to 36 hours.

```
[Switch] password-control update-interval 36
```

Specify that a user can log in five times within 60 days after the password expires.

```
[Switch] password-control expired-user-login delay 60 times 5
```

Set the maximum account idle time to 30 days.

```
[Switch] password-control login idle-time 30
```

Refuse any password that contains the username or the reverse of the username.

```
[Switch] password-control complexity user-name check
```

Specify that no character can appear three or more times consecutively in a password.

```
[Switch] password-control complexity same-character check
```

Add a device management user named **telnet-user**.

```
[Switch] local-user telnet-user class manage
New local user added.
```

Set the service type of the user to **Telnet**.

```
[Switch-luser-manage-telnet-user] service-type telnet
```

Remove the pre-defined user role for **telnet-user**, and use only the authorized user role **level-0**.

```
[Switch-luser-manage-telnet-user] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnet-user] authorization-attribute user-role level-0
```

Set the minimum password length to 20 for the local user.

```
[Switch-luser-manage-telnet-user] password-control length 20
```

Specify that the password of the local user must contain at least four character types and at least four characters for each type.

```
[Switch-luser-manage-telnet-user] password-control composition type-number 4 type-length
4
```

Add a device management user named **ftp-user**.

```
[Switch] local-user ftp-user class manage
```

Set the service type of the user to **FTP**.

```
[Switch-luser-manage-ftp-user] service-type ftp
```

Remove the pre-defined user role for **ftp-user**, and use only the authorized user role **level-9**.

```
[Switch-luser-manage-ftp-user] undo authorization-attribute user-role network-operator
[Switch-luser-manage-ftp-user] authorization-attribute user-role level-9
```

Set the minimum password length to 24 for the local user.

```
[Switch-luser-manage-ftp-user] password-control length 24
```

Specify that the password of the local user must contain at least four character types and at least five characters for each type.

```
[Switch-luser-manage-ftp-user] password-control composition type-number 4 type-length 5
```

Set the password for the local user to expire after one day.

```
[Switch-luser-manage-ftp-user] password-control aging 1
```

Verifying the configuration

Display the global password control configuration.

```
<Switch> display password-control
 Global password control configurations:
 Password control:                   Enabled
 Password aging:                     Enabled (30 days)
 Password length:                    Enabled (10 characters)
 Password composition:               Enabled (1 types,  1 characters per type)
 Password history:                   Enabled (max history records:4)
```

```
 Early notice on password expiration: 7 days
 Maximum login attempts:              2
 Action for exceeding login attempts: Lock
 Minimum interval between two updates:36 hours
 User account idle time:              30 days
 Logins with aged password:           5 times in 60 days
 Password complexity:                 Enabled (username checking)
                                      Disabled (repeated characters checking)
```

Display the password control configuration for local users.

```
<Switch> system-view
[Switch] local-user telnet-user class manage
[Switch-luser-manage-telnet-user] display this
#
local-user telnet-user class manage
 service-type telnet
 authorization-attribute user-role level-0
 password-control length 20
 password-control composition type-number 4 type-length 4
#
return
[Switch-luser-manage-telnet-user] quit
[Switch] local-user ftp-user class manage
[Switch-luser-manage-ftp-user] display this
#
local-user ftp-user class manage
 service-type ftp
 authorization-attribute user-role level-9
 password-control aging 1
 password-control length 24
 password-control composition type-number 4 type-length 5
#
return
```

Verify that you can configure a password that complies with the password control policy for the local user **telnet-user** in interactive mode. In this example, set the password **12345ABGFTweuix@#$%!** for the user.

```
[Switch] local-user telnet-user class manage
[Switch-luser-manage-telnet-user] password
Password:
Confirm :
Updating user information. Please wait ... ...
[Switch-luser-manage-telnet-user] quit
```

Verify that you can configure a password that complies with the password control policy for the local user **ftp-user** in interactive mode. In this example, set the password **123456789ABGFTweuix@#$%!** for the user.

```
[Switch] local-user ftp-user class manage
[Switch-luser-manage-ftp-user] password
Password:
Confirm :
```

```
Updating user information. Please wait ... ...
[Switch-luser-manage-ftp-user] quit
```

Verify that you can use the user accounts to log in to the device and obtain the specified user role for each user account.

Configuration files

```
#
 ftp server enable
#
 telnet server enable
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
#
 password-control enable
 password-control aging 30
 password-control login-attempt 2 exceed lock
 password-control update-interval 36
 password-control login idle-time 30
 password-control expired-user-login delay 60 times 5
 password-control complexity user-name check
 password-control complexity same-character check
#
local-user ftp-user class manage
 service-type ftp
 authorization-attribute user-role level-9
 password-control aging 1
 password-control length 24
 password-control composition type-number 4 type-length 5
#
local-user telnet-user class manage
 service-type telnet
 authorization-attribute user-role level-0
 password-control length 20
 password-control composition type-number 4 type-length 4
#
```

PIM configuration examples

This chapter provides PIM configurations examples.

General configuration restrictions and guidelines

All the interfaces on a switch must operate in the same PIM mode.

Example: Configuring PIM-DM

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 159:

- All the switches are Layer 3 switches.
- 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 159 Network diagram

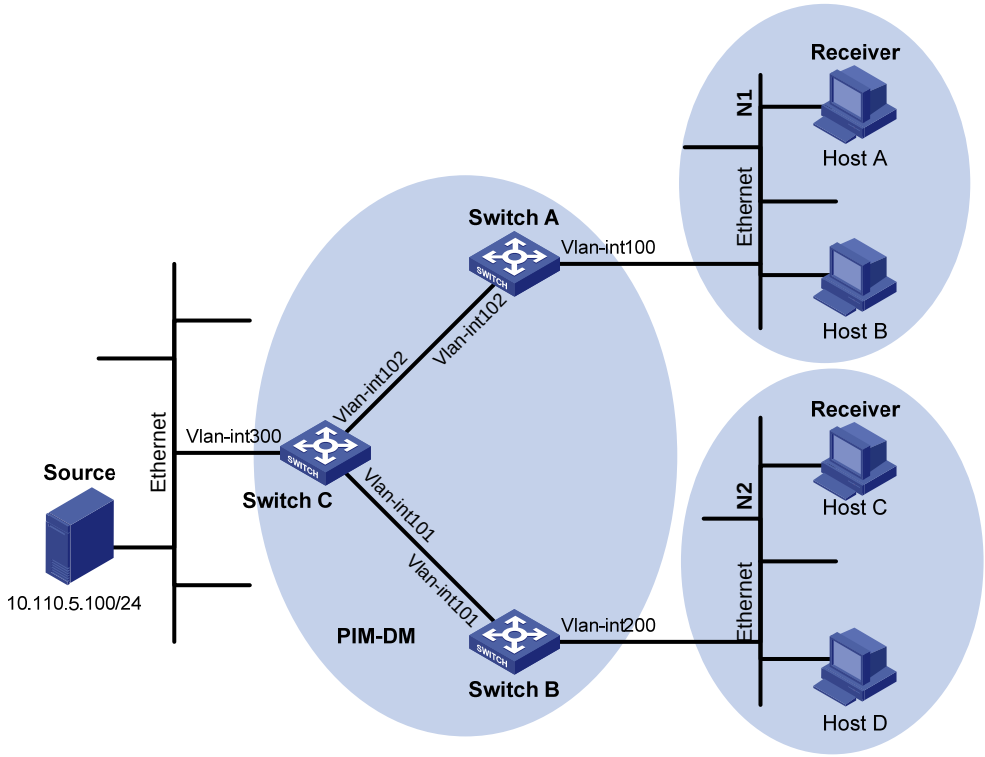


Table 18 Interface and IP address assignment

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 18. (Details not shown.)
2. Configure OSPF on the switches in the PIM-DM domain to make sure the following requirements are met: (Details not shown.)
   - The switches are interoperable at the network layer.

- The switches can dynamically update their routing information.

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

Send IGMPv3 reports from Host A and Host C to join the multicast group **225.1.1.1.** (Details not shown.)

Send multicast data from the multicast source **10.110.5.100/24** to the multicast group **225.1.1.1**. (Details not shown.)

Display information about the PIM routing table on Switch C.

```
[SwitchC] display pim routing-table
 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: Vlan101
             Protocol: pim-dm, UpTime: 00:03:27, Expires: -
         2: Vlan102
             Protocol: pim-dm, UpTime: 00:03:27, Expires: -
```

Display information about the PIM routing table on Switch A.

```
[SwitchA] display pim routing-table
 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: Vlan100
                  Protocol: igmp, UpTime: 00:04:25, Expires: -

 (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: Vlan100
                  Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

Display information about the PIM routing table on Switch B.

```
[SwitchB] display pim routing-table
 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: Vlan200
                  Protocol: igmp, UpTime: 00:04:25, Expires: -

 (10.110.5.100, 225.1.1.1)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:06:14
     Upstream interface: Vlan-interface101,
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information:
       Total number of downstreams: 1
           1: Vlan200
                  Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

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.
 pim dm
 igmp enable
#
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
 pim dm
 igmp enable
#
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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 160:

- All the switches are Layer 3 switches.
- 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 160 Network diagram

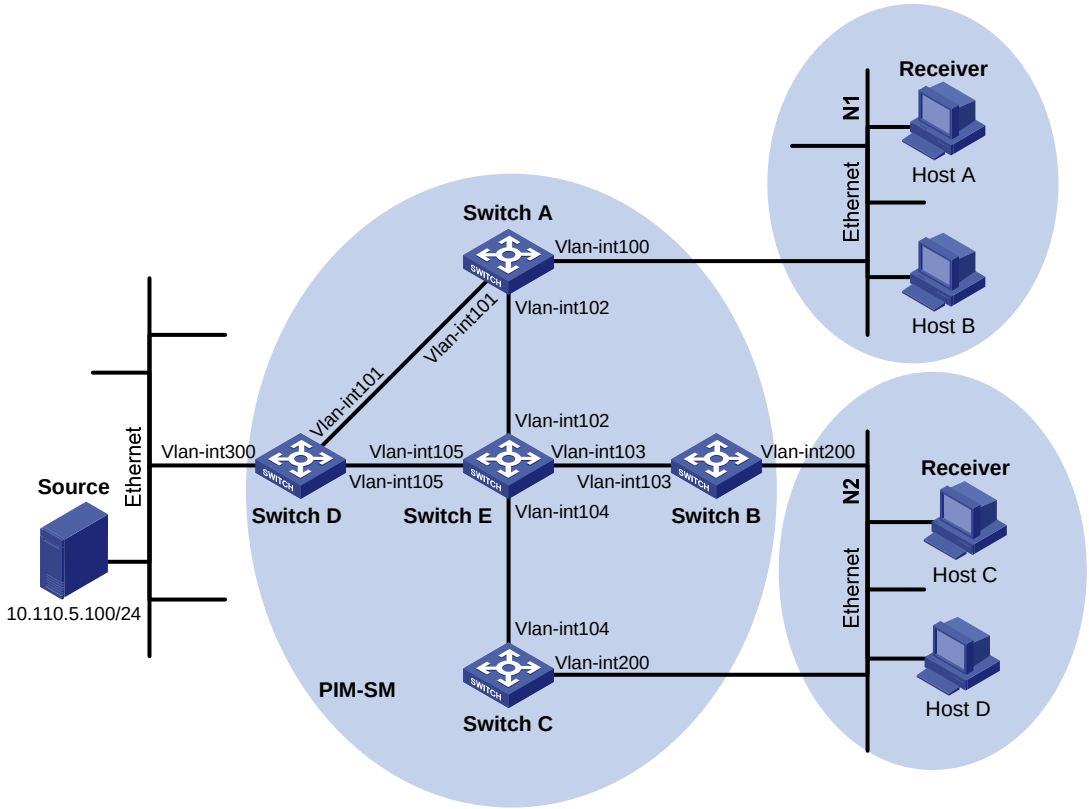


Table 19 Interface and IP address assignment

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

To meet the network requirements, you must perform the following tasks:

- 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 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:

- On a shared-media network with multiple Layer 3 switches connected, you can configure IGMP and PIM-SM on each Layer 3 switch to avoid communication interruption. 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 19. (Details not shown.)
2. Enable OSPF on all switches on the PIM-SM network to make sure the following requirements are met: (Details not shown.)
   - The switches are interoperable at the network layer.
   - The switches can dynamically update their routing information.
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 connects 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-BSR, and set its hash mask length to 32 and priority to 10.

```
[SwitchD] pim
[SwitchD-pim] c-bsr 192.168.4.2 hash-length 32 priority 10
```

   # 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] c-rp 192.168.4.2 group-policy 2005
[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 102 as a as a C-BSR, and set its hash mask length to 32 and priority to 20.

```
[SwitchE] pim
[SwitchE-pim] c-bsr 192.168.9.2 hash-length 32 priority 20
```

   # On Switch E, configure VLAN-interface 102 as a C-RP. Reference ACL 2005 to provide services for only the multicast groups in the range of **225.1.1.0/24**.

```
[SwitchE-pim] c-rp 192.168.9.2 group-policy 2005
[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 IGMP querier information on Switch B.

```
[SwitchB] display igmp interface
 Vlan-interface200(10.110.2.1):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
```

```
    Other querier present time for IGMP: 255s
    Maximum query response time for IGMP: 10s
    Querier for IGMP: 10.110.2.1 (This router)
  IGMP groups reported in total: 1
```

Display IGMP querier information on Switch C.

```
[SwitchC] display igmp interface
 Vlan-interface200(10.110.2.2):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Querier for IGMP: 10.110.2.1
  IGMP groups reported in total: 1
```

The output shows that Switch B is elected as 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
 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
 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 as 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**. (Details not shown.)
   b. Send multicast data from the multicast source **10.110.5.100** to the multicast group **225.1.1.1**. (Details not shown.)
   c. Display PIM routing table information on the switches. Switches A, D, and E are used as examples.

      # Display information about the PIM routing table on Switch A.

      ```
      [SwitchA] display pim routing-table
       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: Vlan100
                 Protocol: igmp, UpTime: 00:13:46, Expires: -

 (10.110.5.100, 225.1.1.1)
    RP: 192.168.9.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: 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: Vlan100
                 Protocol: pim-sm, UpTime: 00:00:42, Expires: -
```

Display information about the PIM routing table on Switch D.

```
[SwitchD] display pim routing-table
 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: Vlan101
                 Protocol: pim-sm, UpTime: 00:00:42, Expires: -
```

Display information about the PIM routing table on Switch E.

```
[SwitchE] display pim routing-table
 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: Vlan102
                 Protocol: pim-sm, UpTime: 00:13:16, Expires: -

 (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
 pim sm
 ip address 10.110.1.1 255.255.255.0
 igmp enable
#
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
 pim sm
 igmp enable
#
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
 pim sm
 igmp enable
#
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 192.168.4.2 priority 10 hash-length 32
 c-rp 192.168.4.2 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 192.168.9.2 priority 20 hash-length 32
 c-rp 192.168.9.2 group-policy 2005#
```

Example: Configuring PIM-SM admin-scoped zones

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 161:

- All switches are Layer 3 switches.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.

Use the PIM-SM administrative scoping mechanism to meet the following requirements:

- 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 and **Source 2** in admin-scoped zone 2 send 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 161 Network diagram

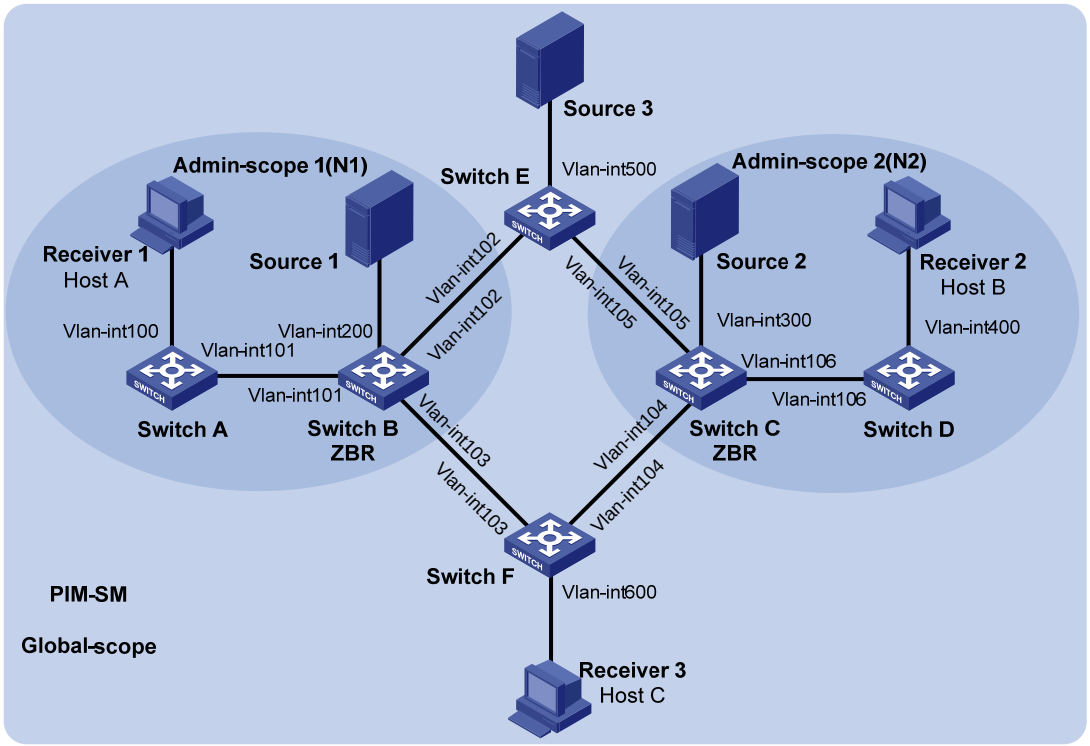


Table 20 Interface and IP address assignment

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	—	192.168.2.10/24
Switch C	VLAN-interface 105	10.110.5.1/24	Source 2	—	192.168.3.10/24
Switch C	VLAN-interface 106	10.110.6.1/24	Source 3	—	192.168.5.10/24
Switch D	VLAN-interface 400	192.168.4.1/24			

Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Configure the boundaries of each admin-scoped zone on the interfaces through which it connects other zones. Make the configuration based on configure the boundaries of each admin-scoped zone on the interfaces through which it connects other zones.
- To make the admin-scoped zones and the global-scoped zone 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.
- 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 20. (Details not shown.)
2. Enable OSPF on all the switches on the PIM-SM network to make sure the following requirements are met: (Details not shown.)
   - The switches are interoperable at the network layer.
   - The switches can dynamically update their routing information.
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
   ```

   # On Switches B, C, D, E, and F, enable IP multicast routing, administrative scoping, and PIM-SM in the same way Switch A is configured. (Details not shown.)
4. Enable IGMP on the interfaces that connects to the receiver hosts:

   # 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.)

5. 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
```

6. 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-BSR and a C-RP for the admin-scoped zone 1.

```
[SwitchB] pim
[SwitchB-pim] c-bsr 10.110.1.2 scope 239.0.0.0 8
[SwitchB-pim] c-rp 10.110.1.2 group-policy 2001
[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-BSR and a C-RP for the admin-scoped zone 2.

```
[SwitchC] pim
[SwitchC-pim] c-bsr 10.110.6.1 scope 239.0.0.0 8
[SwitchC-pim] c-rp 10.110.6.1 group-policy 2001
[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 10.110.2.2
[SwitchE-pim] c-rp 10.110.2.2
[SwitchE-pim] quit
```

Verifying the configuration

1. Verify that the BSR has been elected and the local C-RP configuration in each zone has taken effect:

   # Display BSR information on Switch B.

```
[SwitchB] display pim bsr-info
   Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.2.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

   Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 10.110.1.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:04:54
     Candidate BSR address: 10.110.1.2
       Priority: 64
       Hash mask length: 30
```

   # Display BSR information on Switch C.

```
[SwitchC] display pim bsr-info
   Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.2.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

   Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 10.110.6.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:04:54
     Candidate BSR address: 10.110.6.1
       Priority: 64
       Hash mask length: 30
```

Display BSR information on Switch E.

```
[SwitchE] display pim bsr-info
   Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.2.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

   Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 10.110.2.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:04:54
     Candidate BSR address: 10.110.2.2
       Priority: 64
       Hash mask length: 30
```

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
   BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.2.2               192       150       00:03:39  00:01:51
   Scope: 239.0.0.0/8
     Group/MaskLen: 239.0.0.0/8
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.1.2 (local)       192       150       00:07:44  00:01:51
```

Display RP information on Switch C.

```
[SwitchC] display pim rp-info
   BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.2.2               192       150       00:03:39  00:01:51
   Scope: 239.0.0.0/8
     Group/MaskLen: 239.0.0.0/8
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.6.1 (local)       192       150       00:07:44  00:01:51
```

Display RP information on Switch E.

```
[SwitchE] display pim rp-info
   BSR RP information:
   Scope: non-scoped
```

```
    Group/MaskLen: 224.0.0.0/4
      RP address                Priority  HoldTime  Uptime    Expires
      10.110.2.2(local)         192       150       00:03:39  00:01:51
```

Display RP information on Switch F.

```
[SwitchF] display pim rp-info
   BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address                Priority  HoldTime  Uptime    Expires
       10.110.2.2                192       150       00:03:39  00:01:51
```

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
 pim sm
 igmp enable
#
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
#
```

- 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 10.110.1.2 scope 239.0.0.0 255.0.0.0
 c-rp 10.110.1.2 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 10.110.6.1 scope 239.0.0.0 255.0.0.0
 c-bsr group 239.0.0.0 255.0.0.0
#
```

- 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
 pim sm
 igmp enable
#
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
#
```

- 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 10.110.2.2
 c-rp 10.110.2.2
#
```

- 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
 pim sm
 igmp enable
#
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
#
```

Port isolation configuration examples

This chapter provides port isolation configuration examples.

Example: Configuring port isolation

Applicable product matrix

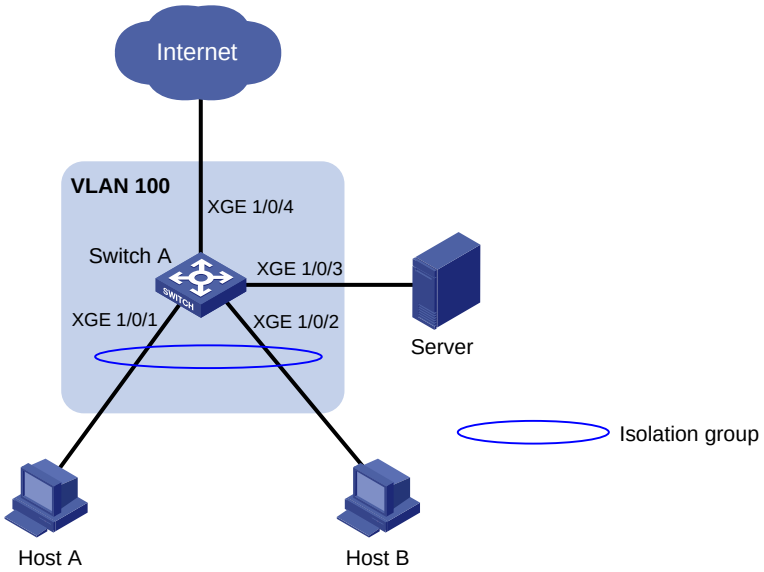
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 162, 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 162 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 Ten-GigabitEthernet 1/0/1, Ten-GigabitEthernet 1/0/2, Ten-GigabitEthernet 1/0/3, and Ten-GigabitEthernet 1/0/4 to the VLAN.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[SwitchA-vlan100] quit
```

Create isolation group 2.

```
[SwitchA] port-isolate group 2
```

Assign ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to the isolation group.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port-isolate enable group 2
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port-isolate enable group 2
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about the isolation group.

```
<SwitchA> display port-isolate group
 Port isolation group information:
 Group ID: 2
 Group members:
    Ten-GigabitEthernet1/0/1
    Ten-GigabitEthernet1/0/2
```

Configuration files

```
#
vlan 100
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
 port-isolate enable group 2
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 port-isolate enable group 2
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/4
 port access vlan 100
#
```

Example: Implementing time-based access control for isolated ports

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

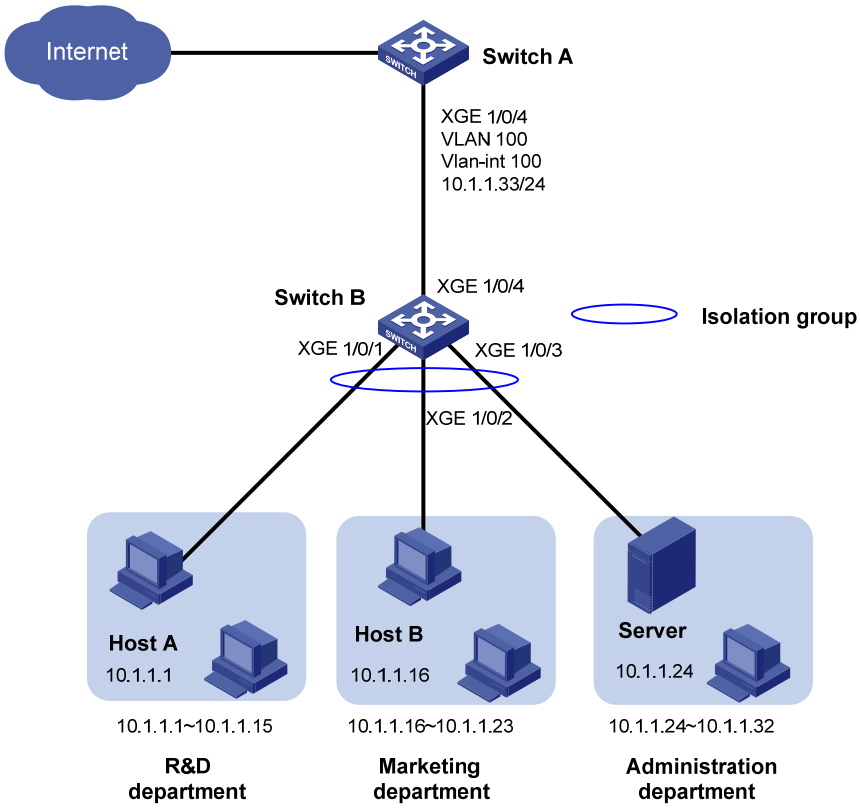
Network requirements

As shown in Figure 163, 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 the 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 time are denied.

Figure 163 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- 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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to VLAN 100.

   ```
   <SwitchB> system-view
   [SwitchB] vlan 100
   [SwitchB-vlan100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
   [SwitchB-vlan100] quit
   ```

   # Assign ports Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/3 to the isolation group to disable host A and host B from accessing the server at Layer 2.

   ```
   [SwitchB] port-isolate group 2
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] port-isolate enable group 2
   [SwitchB-Ten-GigabitEthernet1/0/1] quit
   [SwitchB] interface ten-gigabitethernet 1/0/2
   [SwitchB-Ten-GigabitEthernet1/0/2] port-isolate enable group 2
   [SwitchB-Ten-GigabitEthernet1/0/2] quit
   [SwitchB] interface ten-gigabitethernet 1/0/3
   [SwitchB-Ten-GigabitEthernet1/0/3] port-isolate enable group 2
   [SwitchB-Ten-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 ten-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 periodic time ranges **trname_1** and **trname_2**.

   ```
   [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 Ten-GigabitEthernet 1/0/4 to filter incoming packets.

```
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] packet-filter 3000 inbound
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

Verifying the configuration

1. On Switch B:

Display information about the isolation group.

```
[SwitchB]display port-isolate group
 Port-isolate group information:
 Group ID: 2
 Group members:
    Ten-GigabitEthernet1/0/1
    Ten-GigabitEthernet1/0/2
    Ten-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(Active)
 rule 5 permit ip source 10.1.1.16 0 destination 10.1.1.24 0 time-range
trname_2(Active)
 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 Ten-GigabitEthernet1/0/1
port access vlan 100
 port-isolate enable group 2
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 100
 port-isolate enable group 2
#
interface Ten-GigabitEthernet1/0/3
port access vlan 100
 port-isolate enable group 2
#
interface Ten-GigabitEthernet1/0/4
port access vlan 100
#
```

- Switch A:

```
#
 time-range trname_1 08:00 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 Ten-GigabitEthernet1/0/4
 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 manually enable 802.1X or MAC authentication, change the access control mode, or 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 the smaller value from the following values:
  - The maximum number of secure MAC addresses that port security allows.
  - The maximum number of concurrent users the authentication mode in use allows.

  For example, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses on the port in userLoginSecureExt mode, port security's limit takes effect.

Example: Configuring autoLearn mode

Applicable product matrix

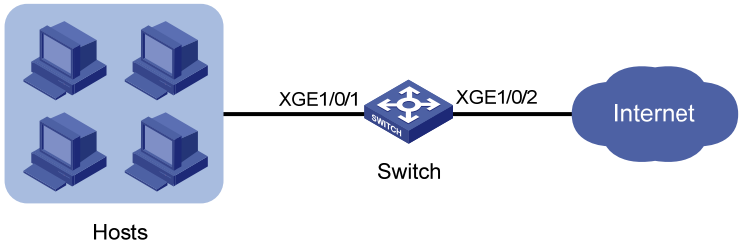
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 164, 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 to access the Internet.

Figure 164 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Configure the autoLearn mode on the access port, Ten-GigabitEthernet 1/0/1.
- Configure an aging timer for the secure MAC addresses, so the switch can update its secure MAC address table. By default, the secure MAC addresses do not age out.
- Configure the port to shut down temporarily for 30 seconds when it receives illegal frames, so the switch can deny any new users to access the Internet after the number of online users reaches 64.

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, you must use the **undo port-security port-mode** command to set the port in noRestrictions mode first.
- Before you enable the autoLearn mode, set 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

Enable port security.

```
<Switch> system-view
[Switch] port-security enable
```

Set the secure MAC aging timer to 30 minutes.

```
[Switch] port-security timer autolearn aging 30
```

Set port security's limit on the number of secure MAC addresses to 64 on port Ten-GigabitEthernet 1/0/1.

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to **autoLearn**.

```
[Switch-Ten-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-Ten-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-Ten-GigabitEthernet1/0/1] quit
[Switch] port-security timer disableport 30
```

Verifying the configuration

Display the port security configuration.

```
[Switch] display port-security interface ten-gigabitethernet 1/0/1
 Port security is enabled globally
 AutoLearn aging time is 30 minutes
 Disableport Timeout: 30s
 OUI value:

Ten-GigabitEthernet1/0/1 is link-up
   Port mode: autoLearn
   NeedToKnow mode: Disabled
   Intrusion protection mode: DisablePortTemporarily
   Max number of secure MAC addresses: 64
   Current number of secure MAC addresses: 0
   Authorization is permitted
```

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 **Current number of secure MAC addresses** field.

Use the **display this** command in interface view to display additional information about the learned MAC addresses.

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] display this
#
interface Ten-GigabitEthernet1/0/1
 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. The port security mode is changed to **secure**. When a frame with an unknown MAC address arrives, intrusion protection is triggered. (Details not shown.)

Use the **display interface** command. The output shows that the port is disabled.

```
[Switch-Ten-GigabitEthernet1/0/1] display interface ten-gigabitethernet 1/0/1
 Ten-GigabitEthernet1/0/1 current state: DOWN (  Port Security Disabled  )
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8927-ad7d
 Description: Ten-GigabitEthernet1/0/1 Interface ......
```

Use the **display interface** command after 30 seconds. The output shows that the interface is enabled.

```
[Switch-Ten-GigabitEthernet1/0/1] display interface ten-gigabitethernet 1/0/1
 Ten-GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: Ten-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 timer autolearn aging 30
 port-security timer disableport 30
#
interface Ten-GigabitEthernet1/0/1
 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 5920	Release 2208P01
HP 5900	Release 2210

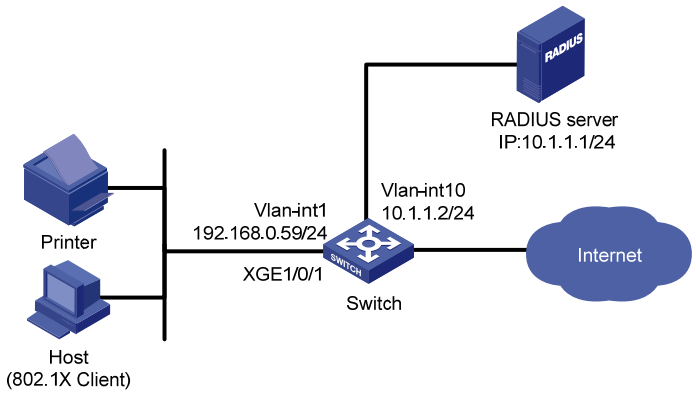
Network requirements

As shown in Figure 165, 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 adds the source MAC addresses of illegal frames to the blocked MAC addresses list. It discards all frames sourced from the blocked MAC addresses.

Figure 165 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Configure the userLoginWithOUI mode on the access port, Ten-GigabitEthernet 1/0/1.
- Add the printer's OUI to the port security module of the switch, so the switch permits the printer to access the Internet. To match the OUIs of different printer vendors, add multiple OUIs to the switch.
- Configure a RADIUS scheme and specify an authentication domain, so the switch can perform RADIUS-based authentication.

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, you must use the **undo port-security port-mode** command to set the port in noRestrictions mode first.
- Specify the authentication port as **1645** in the RADIUS scheme on the access device when an HP device functions as the RADIUS authentication server.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. The server runs the Comware V5 software image. For more information about configuring the RADIUS server, see *HP 5500 HI Series Switches Configuration Guide*.

Configuring IP addresses

Assign an IP address to each interface, as shown in Figure 165. 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. Configure the authentication port as 1645. Set the shared key for authentication to **aabbcc** in plain text.

```
[Switch-radius-radsun] primary authentication 10.1.1.1 1645 key simple 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
```

Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication and authorization of all LAN 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. By default, the authentication method for 802.1X is CHAP.

```
[Switch] dot1x authentication-method chap
```

3. Configure port security:

Add five OUI values.

```
[Switch] port-security oui index 1 mac-address 1234-0100-1111
[Switch] port-security oui index 2 mac-address 1234-0200-1111
[Switch] port-security oui index 3 mac-address 1234-0300-1111
[Switch] port-security oui index 4 mac-address 1234-0400-1111
[Switch] port-security oui index 5 mac-address 1234-0500-1111
```

Set the port security mode to **userLoginWithOUI**.

```
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

Configure port Ten-GigabitEthernet 1/0/1 to perform the **blockmac** intrusion protection feature.

```
[Switch-Ten-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
[Switch-Ten-GigabitEthernet1/0/1] quit
```

Enable port security.

```
[Switch] port-security enable
```

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
```

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
RADIUS Scheme Name  : radsun
  Index : 1
  Primary Auth Server:
    IP: 10.1.1.1                                  Port: 1645   State: active
    VPN : Not configured
Primary Acct Server:
    IP  : Not Configured                            Port: 1813   State: Block
    VPN : Not configured

  Accounting-On function                     : Disabled
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 5
  Retransmission Times                       : 5
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(minutes)      : 12
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : without-domain
```

Display the configuration of the ISP domain **sun**.

```
[Switch] display domain sun
Domain:sun
 State: Active
 Access-limit: Disable
 Access-Count: 0
 default Authentication Scheme:  radius: radsun
 default Authorization  Scheme:  radius: radsun
 default Accounting     Scheme:  none
```

Display the port security configuration.

```
[Switch] display port-security interface ten-gigabitethernet 1/0/1
Port security is enabled globally
 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

 Ten-GigabitEthernet1/0/1 is link-up
   Port mode: userLoginWithOUI
```

```
   NeedToKnow mode: Disabled
   Intrusion protection mode: BlockMacAddress
   Max number of secure MAC addresses: Not configured
   Current number of secure MAC addresses: 0
   Authorization is permitted
```

After an 802.1X user goes online, the number of secure MAC addresses saved by the port is 1.

Display 802.1X information.

```
[Switch] display dot1x interface ten-gigabitethernet 1/0/1
 802.1X protocol is enabled globally
 CHAP authentication is enabled
Configuration: Transmit Period    30 s,  Handshake Period       15 s
               Quiet Period       60 s,  Quiet Timer is disabled
               Supp Timeout       30 s,  Server Timeout        100 s
               Reauth Period   3600 s
               Max attempts for sending an authentication request    2
 Max number of 802.1X users is 1024 per slot
 Current number of online 802.1X users is 1

 Ten-GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Handshake is enabled
   Handshake secure is disabled
   802.1X unicast-trigger is disabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication mode is Auto
   Port access control type is MAC-based
   802.1X multicast-trigger is enabled
   Mandatory authentication domain: Not configured
   Max online users is 256

   EAPOL Packets: 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 Users: 1
```

The port also allows an additional user whose MAC address has an OUI from the specified OUIs to pass authentication.

Display the MAC address information for interface Ten-GigabitEthernet 1/0/1.

```
[Switch] display mac-address interface ten-gigabitethernet 1/0/1
```

```
MAC Address     VLAN ID   State          Port/NickName                 Aging
1234-0300-0011  1         Learned        Ten-GigabitEthernet1/0/1        Y
```

Configuration files

```
#
 port-security enable
 port-security oui index 1 mac-address 1234-0100-0000
 port-security oui index 1 mac-address 1234-0200-0000
 port-security oui index 1 mac-address 1234-0300-0000
 port-security oui index 1 mac-address 1234-0400-0000
 port-security oui index 1 mac-address 1234-0500-0000
#
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
#
interface Ten-GigabitEthernet1/0/1
 port-security port-mode userlogin-withoui
 port-security intrusion-mode blockmac
#
```

Example: Configuring macAddressOrUserLoginSecure mode

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

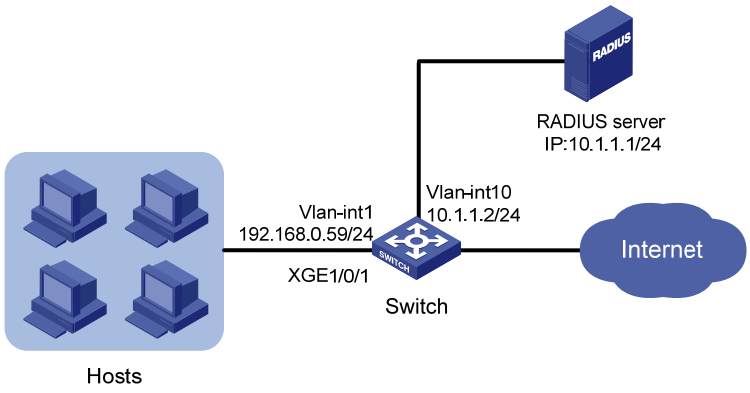
Network requirements

As shown in Figure 166, the switch uses the RADIUS server to authenticate users.

Configure port security mode **macAddressOrUserLoginSecure** on the switch to meet the following requirements:

- Allows only one 802.1X user to pass authentication, and allows multiple MAC authentication users to pass authentication.
- Uses shared user account with username **aaa** and password **123456** for MAC authentication users.
- Allows a maximum of 64 authenticated users.
- Performs the **ntkonly** feature to prevent frames from being sent to unknown MAC addresses.

Figure 166 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Configure the macAddressOrUserLoginSecure mode on the access port, Ten-GigabitEthernet 1/0/1.
- Configure a RADIUS scheme and specify an authentication domain, so the switch can perform RADIUS-based authentication.

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, you must use the **undo port-security port-mode** command to set the port in noRestrictions mode first.
- Specify the authentication port as **1645** in the RADIUS scheme on the access device when an HP device functions as the RADIUS authentication server.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. The server runs the Comware V5 software image. For more information about configuring the RADIUS server, see *HP 5500 HI Series Switches Configuration Guide*.

Configuring IP addresses

Assign an IP address to each interface, as shown in Figure 166. 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. Configure the authentication port as 1645. Set the shared key for authentication to **aabbcc** in plain text.

   ```
   [Switch-radius-radsun] primary authentication 10.1.1.1 1645 key simple 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
   ```

   # Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication and authorization of all LAN 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. By default, the authentication method for 802.1X is CHAP.

   ```
   [Switch] dot1x authentication-method chap
   ```

   # 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 port security's limit on the number of secure MAC addresses to 64 on Ten-GigabitEthernet 1/0/1.

   ```
   [Switch] interface ten-gigabitethernet 1/0/1
   [Switch-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
   ```

   # Set the port security mode to **macAddressOrUserLoginSecure**.

   ```
   [Switch-Ten-GigabitEthernet1/0/1] port-security port-mode userlogin-secure-or-mac
   ```

   # Set the NTK mode of the port to **ntkonly**.

   ```
   [Switch-Ten-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
   [Switch-Ten-GigabitEthernet1/0/1] quit
   ```

   # Enable port security.

   ```
   [Switch] port-security enable
   ```

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
```

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 ten-gigabitethernet 1/0/1
 Port security is enabled globally
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:

 Ten-GigabitEthernet1/0/1 is link-up
   Port mode: macAddressOrUserLoginSecure
   NeedToKnow mode: NeedToKnowOnly
   Intrusion protection mode: NoAction
   Max number of secure MAC addresses: 64
   Current number of secure MAC addresses: 0
   Authorization is permitted
```

Display MAC authentication information.

```
[Switch] display mac-authentication interface ten-gigabitethernet 1/0/1
MAC 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
          Max number of users is 1024 per slot
          Current number of online users is 3
          Current authentication domain is sun

Silent MAC User info:
          MAC Addr         VLAN ID  From Port                    Port Index

Ten-GigabitEthernet1/0/1 is link-up
  MAC authentication is enabled
  Max number of online users is 256
  Current number of online users is 32
```

```
  Current authentication domain: Not configured
  Authentication attempts: successful 3, failed 1
          MAC Addr          Auth state
          1234-0300-0011    authenticated
          1234-0300-0012    authenticated
          1234-0300-0013    authenticated
```

Display 802.1X authentication information.

```
[Switch] display dot1x interface ten-gigabitethernet 1/0/1
 802.1X protocol is enabled globally
 CHAP authentication is enabled
Configuration: Transmit Period   30 s,  Handshake Period       15 s
               Quiet Period      60 s,  Quiet Timer is disabled
               Supp Timeout      30 s,  Server Timeout        100 s
               Reauth Period   3600 s
               Max attempts for sending an authentication request    2
 Max number of 802.1X users is 1024 per slot
 Current number of online 802.1X users is 1
Ten-GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Handshake is enabled
   802.1X unicast-trigger is disabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication mode is Auto
   Port access control type is MAC-based
   802.1X multicast-trigger is enabled
   Mandatory authentication domain: Not configured
   Max online users is 256

   EAPOL Packets: 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 Users: 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
#
interface Ten-GigabitEthernet1/0/1
 port-security max-mac-count 64
 port-security port-mode userlogin-secure-or-mac
 port-security ntk-mode ntkonly
#
```

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 5900	Release 2208P01
HP 5920	Release 2210

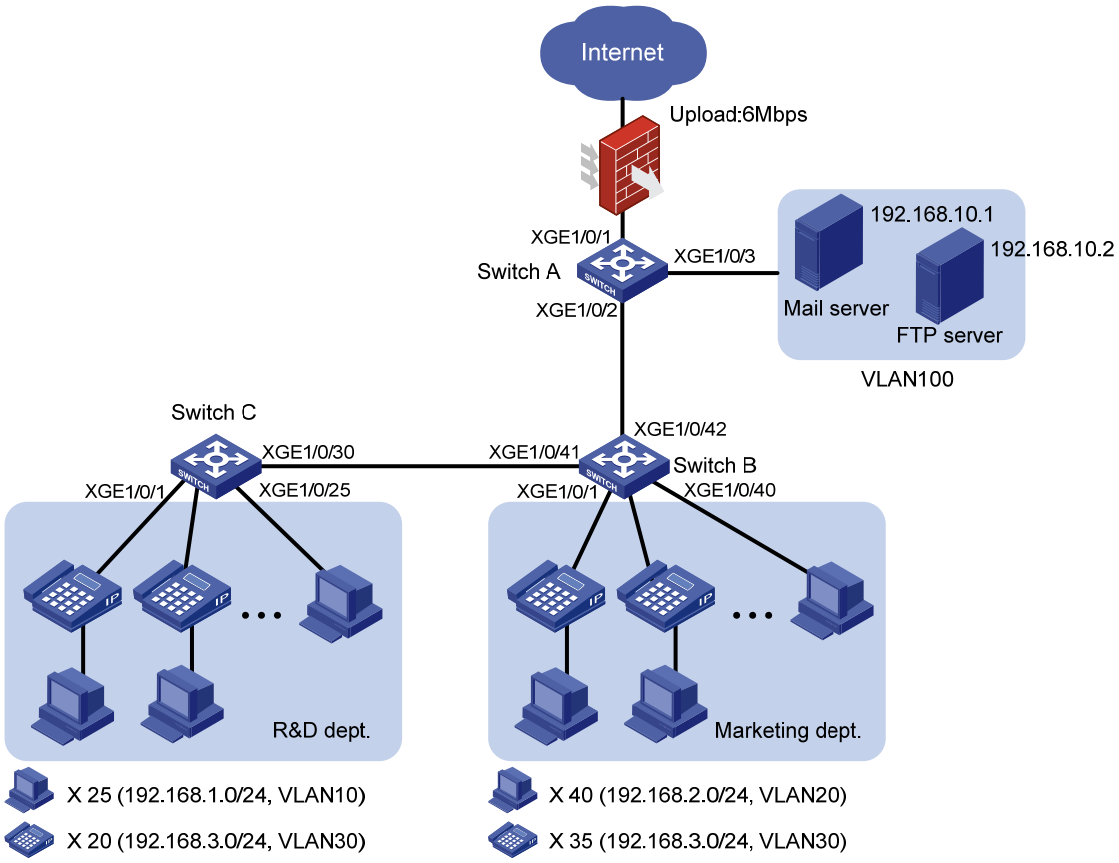
Network requirements

As shown in Figure 167, 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 are making 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 167 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- 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 the following priority marking actions:

- Local precedence marking.
- Drop precedence marking.
- 802.1p priority marking.
- DSCP marking.
- IP precedence marking.

Otherwise, a QoS policy that references the traffic behavior cannot be applied correctly.

Configuration procedures

Configuring Switch A

1. Configure VLAN attributes for the interfaces:

   # Configure Ten-GigabitEthernet 1/0/1 as a trunk port.

   ```
   <SwitchA> system-view
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
   ```

   # Assign the port to VLAN 10, VLAN 20, VLAN 30, and VLAN 100.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 20 30 100
   ```

   # Remove the port from VLAN 1.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Configure Ten-GigabitEthernet 1/0/2 as a trunk port.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
   ```

   # Assign the port to VLAN 10, VLAN 20, and VLAN 30.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10 20 30
   ```

   # Remove the port from VLAN 1.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
   [SwitchA-Ten-GigabitEthernet1/0/2] quit
   ```

   # Create VLAN 100.

   ```
   [SwitchA] vlan 100
   [SwitchA-vlan100] quit
   ```

   # Assign Ten-GigabitEthernet 1/0/3 to VLAN 100 as an access port.

   ```
   [SwitchA] interface gigabitethernet 1/0/3
   [SwitchA-Ten-GigabitEthernet1/0/3] port access vlan 100
   [SwitchA-Ten-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.

   ```
   [SwitchA] traffic behavior rd_http
   [SwitchA-behavior-rd_http] car cir 1024
   [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.

```
[SwitchA] traffic behavior mkt_http
[SwitchA-behavior-mkt_http] car cir 2048
[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 and PIR 800 kbps.

```
[SwitchA] traffic behavior ip_voip
[SwitchA-behavior-ip_voip] car cir 640 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.

```
[SwitchA] traffic behavior email
[SwitchA-behavior-email] car cir 512
[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.

```
[SwitchA] traffic behavior ftp
[SwitchA-behavior-ftp] car cir 1024
[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 Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface Ten-GigabitEthernet1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy http&voice inbound
[SwitchA-Ten-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 Ten-GigabitEthernet 1/0/3.

```
[SwitchA] interface Ten-GigabitEthernet1/0/3
[SwitchA- Ten-GigabitEthernet1/0/3][SwitchA- Ten-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 *HP 5920 & 5900 Switch Series Layer 2—LAN Switch Configuration Guide*.

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 an interface range named **group**, and assign all interfaces that connect to hosts and IP phones to the interface range.

```
<SwitchB> system-view
[SwitchB] interface range name group interface ten-gigabitethernet 1/0/1 to
ten-gigabitethernet 1/0/40
```

Configure the interfaces in the interface range as trunk ports.

```
[SwitchB-if-range-group] port link-type trunk
```

Configure the PVID of these interfaces as VLAN 20.

```
[SwitchB-if-range-group] port trunk pvid vlan 20
```

Assign these interfaces to VLAN 20 and VLAN 30, and remove these interfaces from VLAN 1.

```
[SwitchB-if-range-group] port trunk permit vlan 20 30
[SwitchB-if-range-group] undo port trunk permit vlan 1
[SwitchB-if-range-group] quit
```

Configure Ten-GigabitEthernet 1/0/41 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/41
[SwitchB-Ten-GigabitEthernet1/0/41] port link-type trunk
```

Assign Ten-GigabitEthernet 1/0/41 to VLAN 10 and VLAN 30, and remove it from VLAN 1.

```
[SwitchB-Ten-GigabitEthernet1/0/41] port trunk permit vlan 10 30
[SwitchB-Ten-GigabitEthernet1/0/41] undo port trunk permit vlan 1
[SwitchB-Ten-GigabitEthernet1/0/41] quit
```

Configure Ten-GigabitEthernet 1/0/42 as a trunk port.

```
[SwitchB] interface ten-gigabitethernet 1/0/42
[SwitchB-Ten-GigabitEthernet1/0/42] port link-type trunk
```

Assign it to VLAN 10, VLAN 20, and VLAN 30, and remove it from VLAN 1.

```
[SwitchB-Ten-GigabitEthernet1/0/42] port trunk permit vlan 10 20 30
[SwitchB-Ten-GigabitEthernet1/0/42] undo port trunk permit vlan 1
[SwitchB-Ten-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.

```
[SwitchB] traffic behavior mkt
[SwitchB-behavior-mkt] car cir 256
[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
[SwitchB-qospolicy-mkt] quit
```

Apply the QoS policy **mkt** to the inbound direction of port group 1.

```
[SwitchB] interface range name group
[SwitchB-if-range-group] qos apply policy mkt inbound
```

Configuring Switch C

1. Configure interfaces and VLANs:

Create an interface range named **group**, and assign all interfaces that connect to hosts and IP phones to the interface range.

```
[SwitchC] interface range name group interface Ten-GigabitEthernet 1/0/1 to
Ten-GigabitEthernet 1/0/25
```

Configure the interfaces in port group 1 as trunk ports.

```
[SwitchC-if-range-group] port link-type trunk
```

Configure the PVID of these interfaces as VLAN 10.

```
[SwitchC-if-range-group] port trunk pvid vlan 10
```

Assign these interfaces to VLAN 10 and VLAN 30, and remove these interfaces from VLAN 1.

```
[SwitchC-if-range-group] port trunk permit vlan 10 30
[SwitchC-if-range-group] undo port trunk permit vlan 1
[SwitchC-if-range-group] quit
```

Configure Ten-GigabitEthernet 1/0/30 as a trunk port.

```
[SwitchC] interface ten-gigabitethernet 1/0/30
[SwitchC-Ten-GigabitEthernet1/0/30] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/30] port trunk permit vlan 10 30
```

Assign it to VLAN 10 and VLAN 30, and remove it from VLAN 1.

```
[SwitchC-Ten-GigabitEthernet1/0/30] undo port trunk permit vlan 1
[SwitchC-Ten-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.

```
[SwitchC] traffic behavior rd
[SwitchC-behavior-rd] car cir 128
[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
[SwitchC-qospolicy-rd] quit
```

Apply the QoS policy **rd** to the inbound direction of port group 1.

```
[SwitchC] interface range name group
[SwitchC-if-range-group] qos apply policy rd inbound
```

Configuration files

- Switch A:

```
#
vlan 100
#
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 32256 ebs 512 green pass red discard yellow pass
traffic behavior ip_voice
 car cir 640 cbs 40448 ebs 512 pir 800 green pass red discard yellow pass
traffic behavior ftp
 car cir 1024 cbs 64000 ebs 512 green pass red discard yellow pass
traffic behavior rd_http
 car cir 1024 cbs 64000 ebs 512 green pass red discard yellow pass
traffic behavior mkt_http
 car cir 2048 cbs 128000 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 Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 100
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 10 20 30
 qos apply policy http&voice inbound
#
interface Ten-Ten-GigabitEthernet1/0/3
 port access vlan 100
 qos apply policy email&ftp inbound
```

- Switch B:

```
#
 interface range name group interface Ten-GigabitEthernet1/0/1 to
Ten-GigabitEthernet1/0/40
#
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 16384 ebs 512 green pass red discard yellow pass
#
qos policy mkt
 classifier mkt behavior mkt
#
interface Ten-GigabitEthernet1/0/1
 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 Ten-GigabitEthernet1/0/2
 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 Ten-GigabitEthernet1/0/3
 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 Ten-GigabitEthernet1/0/41
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 10 30
#
interface Ten-GigabitEthernet1/0/42
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
```

- Switch C:

```
#
 interface range name group interface Ten-GigabitEthernet1/0/1 to
Ten-GigabitEthernet1/0/25
#
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 8192 ebs 512 green pass red discard yellow pass
#
qos policy rd
 classifier rd behavior rd
#
interface Ten-GigabitEthernet1/0/1
 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 Ten-GigabitEthernet1/0/2
 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 Ten-GigabitEthernet1/0/3
 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 Ten-GigabitEthernet1/0/30
 port link-type trunk
 undo port trunk permit vlan 1
```

```
port trunk permit vlan 10 30
```

Example: Allocating bandwidth based on VLANs

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

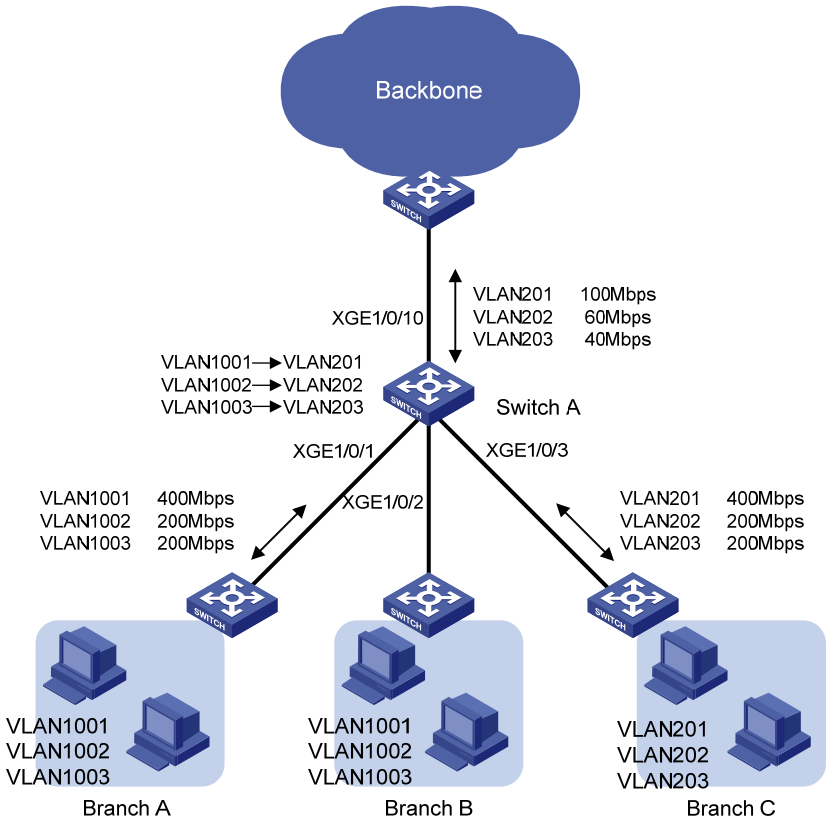
As shown in Table 21Figure 168, Switch A aggregates traffic from the branches and transmits the traffic to the backbone network through a leased line. Each branch site assigns packets of different applications to different VLANs.

- Configure one-to-one VLAN mapping on Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 of Switch A. Traffic from different applications is re-mapped to VLANs as per the transmission scheme on the backbone network.
- Configure traffic policing to allocate bandwidth to traffic from different VLANs, as shown in Table 21.

Table 21 Bandwidth allocation

XGE1/0/1 and XGE1/0/2 (uplink or downlink)			XGE1/0/3 (uplink or downlink)			XGE1/0/10 (uplink or downlink)		
VLAN 1001	VLAN 1002	VLAN 1003	VLAN 201	VLAN 202	VLAN 203	VLAN 201	VLAN 202	VLAN 203
400 Mbps	200 Mbps	200 Mbps	400 Mbps	200 Mbps	200 Mbps	100 Mbps	60 Mbps	40 Mbps

Figure 168 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- To allocate bandwidth based on VLANs, you need to use QoS policies to perform the following tasks:
  - Configure VLAN-based traffic classes.
  - Configure per-VLAN traffic policing behaviors.
  - Associate each class with its specific traffic behavior.
- VLAN mapping is also implemented with QoS policies. Use the following guidelines when 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.
  - Associating the policing action with the class for the original VLAN first renders the VLAN mapping action useless. The device stops searching the QoS policy once a match is found.

Configuration restrictions and guidelines

When you allocate bandwidth based on VLANs, 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 to the port.
- In a traffic behavior, the traffic policing action cannot be configured together with the following priority marking actions:
  - Local precedence marking.
  - Drop precedence marking.
  - 802.1p priority marking.
  - DSCP marking.
  - IP precedence marking.

  Otherwise, a QoS policy that references the 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.

```
[SwitchA] traffic behavior car_vlan201_downlink
[SwitchA-behavior-car_vlan201_downlink] car cir 400000
[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.

```
[SwitchA] traffic behavior car_vlan202_downlink
[SwitchA-behavior-car_vlan202_downlink] car cir 200000
[SwitchA-behavior-car_vlan202_downlink] quit
[SwitchA] traffic behavior car_vlan203_downlink
[SwitchA-behavior-car_vlan203_downlink] car cir 200000
[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 Ten-GigabitEthernet 1/0/3 to rate limit the upstream traffic of VLAN 201, VLAN 202, and VLAN 203 from Branch C.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] qos apply policy downlink_in_c inbound
```

Apply the QoS policy **downlink_in_c** to the outgoing traffic of Ten-GigabitEthernet 1/0/3 to rate limit the downstream traffic of VLAN 201, VLAN 202, and VLAN 203 to Branch C.

```
[SwitchA-Ten-GigabitEthernet1/0/3] qos apply policy downlink_in_c outbound
```

Perform the following configurations:

- Configure Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/10 as trunk ports.
- Assign them to VLANs 201 through 203.
- Remove them from VLAN 1.

```
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 201 to 203
[SwitchA-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
[SwitchA] interface Ten-GigabitEthernet 1/0/10
[SwitchA-Ten-GigabitEthernet1/0/10] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/10] port trunk permit vlan 201 to 203
[SwitchA-Ten-GigabitEthernet1/0/10] undo port trunk permit vlan 1
```

Configuring bandwidth allocation related to VLAN mapping

1. Perform the following configurations:
   - Configure Ten-GigabitEthernet 1/0/1 and Ten-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 Ten-GigabitEthernet1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
   [SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 1001 to 1003 201 to 203
   [SwitchA-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   [SwitchA-Ten-GigabitEthernet1/0/1] qinq enable
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   [SwitchA] interface Ten-GigabitEthernet1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
   [SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 1001 to 1003 201 to 203
   [SwitchA-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
   [SwitchA-Ten-GigabitEthernet1/0/2] qinq enable
   [SwitchA-Ten-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**. The classes and behaviors 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**. The classes and behaviors 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.

Use the following traffic classes:

- VLAN 201: **201_to_1001**.
- VLAN 202: **202_to_1002**.
- VLAN 203: **203_to_1003**.

Use the following behaviors for policing the traffic:

- **car_vlan201_downlink**.
- **car_vlan202_downlink**.
- **car_vlan203_downlink**.

The behaviors are configured in "Configuring bandwidth allocation unrelated to VLAN mapping."

5. Configure classes and behaviors to rate limit 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 named **vlan202_downlink** and **vlan203_downlink**.

```
[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
```

Use the following behaviors:

- **car_vlan201_downlink**.
- **car_vlan202_downlink**.
- **car_vlan203_downlink**.

6. Configure classes and behaviors for rate-limiting the upstream traffic to the backbone network.

Use the following classes:

- **201_to_1001**.
- **202_to_1002**.
- **203_to_1003**.

Create a behavior named **car_vlan201_uplink** for rate limiting the upstream traffic of VLAN 201 on Switch A. Set the CIR to 100000 kbps.

```
[SwitchA] traffic behavior car_vlan201_uplink
[SwitchA-behavior-car_vlan201_uplink] car cir 100000
[SwitchA-behavior-car_vlan201_uplink] quit
```

Create a behavior named **car_vlan202_uplink** for rate limiting upstream traffic of VLAN 202. Set the CIR to 60000 kbps.

```
[SwitchA] traffic behavior car_vlan202_uplink
```

```
[SwitchA-behavior-car_vlan202_uplink] car cir 60000
[SwitchA-behavior-car_vlan202_uplink] quit
```

Create a behavior named **car_vlan203_uplink** for rate limiting upstream traffic of VLAN 203. Set the CIR to 40000 kbps.

```
[SwitchA] traffic behavior car_vlan203_uplink
[SwitchA-behavior-car_vlan203_uplink] car cir 40000
[SwitchA-behavior-car_vlan203_uplink] quit
```

7. Configure classes and behaviors to rate limit the downstream traffic from the backbone network.

   # Use the following classes:

   - **201_to_1001**.
   - **202_to_1002**.
   - **203_to_1003**.

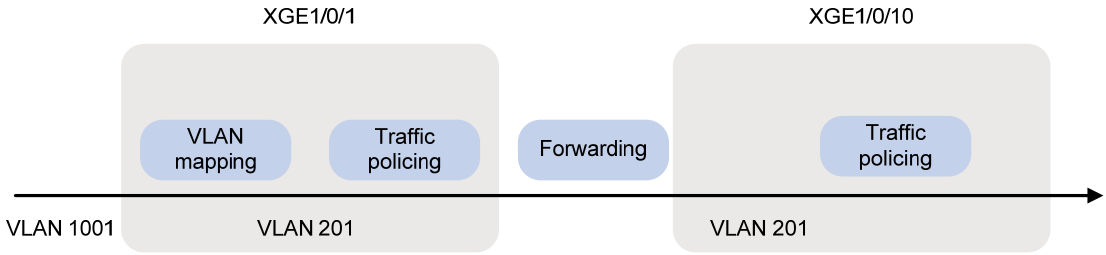
   # Use the following behaviors:

   - **car_vlan201_uplink**.
   - **car_vlan202_uplink**.
   - **car_vlan203_uplink**.

8. Configure and apply the QoS policies for upstream traffic.

   Figure 169 shows how the switches process the upstream traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.

   Figure 169 Upstream traffic processing



   # Create a QoS policy named **downlink_in**, and configure the following class-behavior associations in the following order:

   a. The VLAN mapping class-behavior associations.
   b. 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface Ten-GigabitEthernet1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy downlink_in inbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface Ten-GigabitEthernet1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy downlink_in inbound
[SwitchA-Ten-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
```

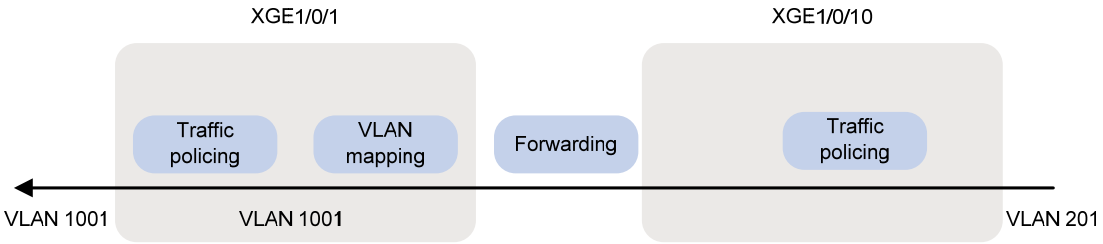
Apply QoS policy **uplink_out** to the outgoing traffic of Ten-GigabitEthernet 1/0/10.

```
[SwitchA] interface Ten-GigabitEthernet1/0/10
[SwitchA-Ten-GigabitEthernet1/0/10] qos apply policy uplink_out outbound
```

9. Configure and apply the QoS policies for downstream traffic.

Figure 170 shows how the switches process the downstream traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.

Figure 170 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 Ten-GigabitEthernet 1/0/10.

```
[SwitchA] interface Ten-GigabitEthernet1/0/10
[SwitchA-Ten-GigabitEthernet1/0/10] qos apply policy uplink_in inbound
```

Create a QoS policy named **downlink_out**, and configure the following class-behavior associations in the following order:

a. The VLAN mapping class-behavior associations.

b. 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 Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface Ten-GigabitEthernet1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy downlink_out outbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface Ten-GigabitEthernet1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy downlink_out outbound
[SwitchA-Ten-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 25000448 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan202_downlink
 car cir 200000 cbs 12500480 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan203_downlink
 car cir 200000 cbs 12500480 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan201_uplink
 car cir 100000 cbs 6250496 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan202_uplink
 car cir 60000 cbs 3750400 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan203_uplink
 car cir 40000 cbs 2500096 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 Ten-GigabitEthernet1/0/1
 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 Ten-GigabitEthernet1/0/2
 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 Ten-GigabitEthernet1/0/10
 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

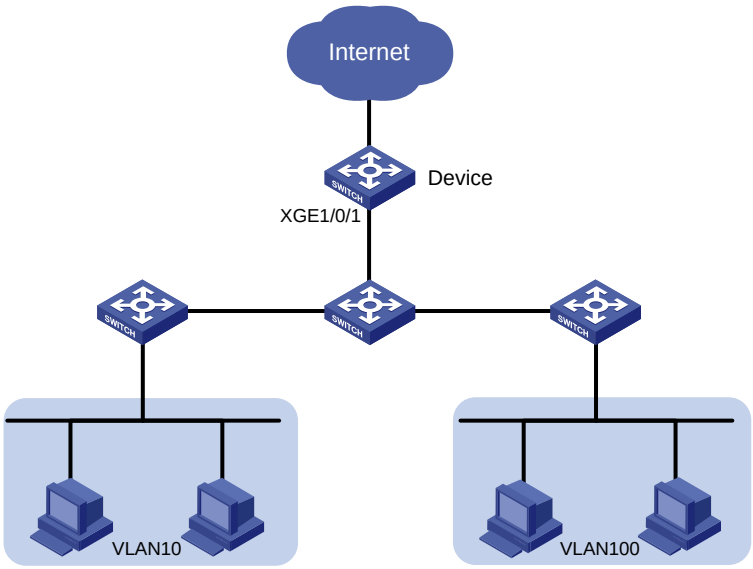
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 171, configure aggregate CAR on Ten-GigabitEthernet 1/0/1 to limit the incoming traffic from VLAN 10 and VLAN 100 to 200 Mbps and to drop the excess traffic.

Figure 171 Network diagram



Configuration restrictions and guidelines

In a traffic behavior, the traffic policing action cannot be configured together with the following priority marking actions:

- Local precedence marking.
- Drop precedence marking.
- 802.1p priority marking.
- DSCP marking.
- IP precedence marking.

Otherwise, a QoS policy that references the behavior cannot be applied correctly.

Configuration procedures

In this example, the access layer devices have added VLAN tags for the traffic of VLAN 10 and VLAN 100 and sent the traffic to Device.

Configure Ten-GigabitEthernet 1/0/1 as a trunk port.

```
<Device> system-view
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port link-type trunk
```

Assign it to VLANs 10 and 100.

```
[Device-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 100
```

Remove it from VLAN 1.

```
[Device-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Device-Ten-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,.

```
[Device] traffic classifier 1
[Device-classifier-1] if-match service-vlan-id 10
[Device-classifier-1] quit
```

Configure a behavior with the aggregate CAR action.

```
[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.

```
[Device] traffic classifier 2
[Device-classifier-2] if-match service-vlan-id 100
[Device-classifier-2] quit
```

Configure a behavior with the aggregate CAR action.

```
[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 Ten-GigabitEthernet 1/0/1.

```
[Device] interface Ten-GigabitEthernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] qos apply policy car inbound
```

Configuration files

```
#
 qos car aggcar-1 aggregative cir 200000 cbs 12500480 ebs 512 green pass yellow pass 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 Ten-GigabitEthernet1/0/1
```

```
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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 172, a company connects its branches (on the left) and its headquarters (on the right) through a dedicated line. The dedicated line transmits the FTP traffic, service application traffic, and IP voice traffic.

Configure traffic policing on the edge device Switch B of the headquarters using the following settings:

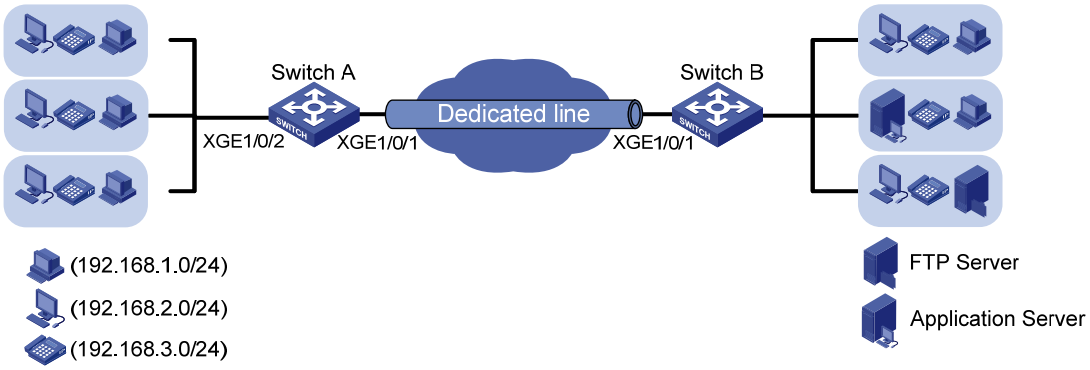
- CIR set to10 Mbps for IP voice traffic.
- CIR set to 3 Mbps for service application traffic.
- CIR set to 7 Mbps for FTP traffic.

Configure traffic shaping on edge device Switch A of the branch to ensure the following actions take place:

- Cooperate with the traffic policing configured in the headquarters.
- Buffer the excess bursty traffic.
- Avoid packet loss.

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 172 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- 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 the same (all use the default value). 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 172 is reachable. Information about implementing connectivity on Switch A and Switch B is not shown (for example, creating VLAN-interfaces and assigning IP addresses to VLAN-interfaces).

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:

   # 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 Ten-GigabitEthernet 1/0/2.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos apply policy shaping inbound
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

After the configuration above, the local precedence values of the three traffic flows are changed, and 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 Ten-GigabitEthernet 1/0/1, and set the CIR to 10000 kbps for queue 6.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos gts queue 6 cir 10000
```

Configure traffic shaping on port Ten-GigabitEthernet 1/0/1, and set the CIR to 3000 kbps for queue 4.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos gts queue 4 cir 3000
```

Configure traffic shaping on port Ten-GigabitEthernet 1/0/1, and set the CIR to 7000 kbps for queue 2.

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos gts queue 2 cir 7000
```

Configuring rate limiting

Configure rate limiting on port Ten-GigabitEthernet 1/0/1, and set the CIR to 20000 kbps for the outgoing traffic of the port.

```
[SwitchA-Ten-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: Ten-GigabitEthernet1/0/1
 Rule(s): If-match queue 6
 CIR 10000 (kbps), CBS 625152 (byte)
 Rule(s): If-match queue 4
  CIR 3000 (kbps), CBS 187904 (Bytes)
 Rule(s): If-match queue 2
  CIR 7000 (kbps), CBS 437760 (Bytes)
```

Use the **display qos lr interface** command to display the rate limiting configuration of a port.

```
<Sysname> display qos lr interface
Interface: Ten-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 Ten-GigabitEthernet1/0/1
 qos lr outbound cir 20000 cbs 1250304
 qos gts queue 6 cir 10000 cbs 625152
 qos gts queue 2 cir 3000 cbs 187904
 qos gts queue 4 cir 7000 cbs 437760
#
interface Ten-GigabitEthernet1/0/2
 qos apply policy shaping inbound
```

Priority and queue scheduling configuration examples

This chapter provides priority mapping, priority marking, and queue scheduling configuration examples.

Example: Configuring priority mapping and queue scheduling

Applicable product matrix

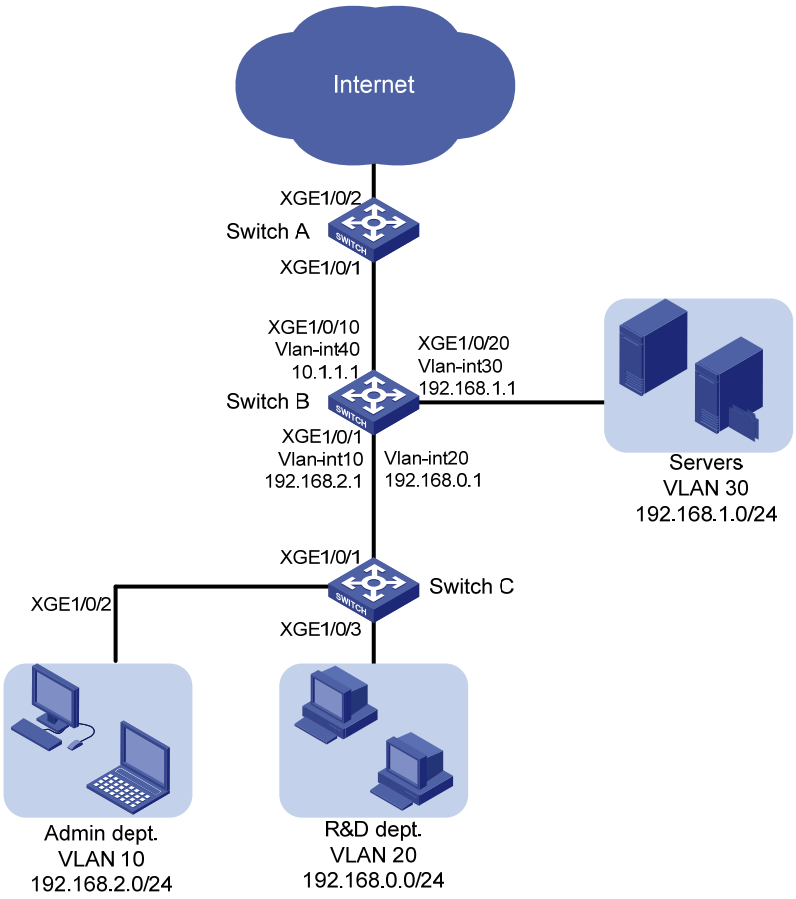
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

The network diagram of a company is shown in Figure 173. Configure priority mapping and queue scheduling to meet the following requirements:

- **Access to the internal server farm**—The traffic from the Administration department takes priority over the traffic 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 the traffic 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.
- The Internet-accessing traffic includes the following types: HTTP, FTP, and Email, with the DSCP values 33, 35, and 27, respectively. The three types of traffic is transmitted 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 173 Network diagram



Requirements analysis

Priority configuration for the internal network traffic

To meet the network requirements, you must perform the following tasks:

- To prioritize packets by department, configure different port priorities for the ports connected to the two departments. The packets from the two departments must be 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. The devices must enqueue packets by 802.1p priority.
- To satisfy the packet scheduling ratio when congestion occurs, configure WRR. Also configure different weights for queues.

Priority configuration for the Internet traffic

To meet the network requirements, you must perform the following tasks:

- To 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.

- To determine the transmission priority based on the upper-layer protocols, configure trusting the DSCP values on the port, so that the port can enqueue packets based on the DSCP values.
- To assign packets with DSCP value 33 to a higher-priority queue, modify the DSCP-to-802.1p priority mapping table to map DSCP value 33 to a higher 802.1p priority value than the default. 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 by default.
- 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 Ten-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 Ten-GigabitEthernet 1/0/2
   [SwitchC-Ten-GigabitEthernet1/0/2] port access vlan 10
   [SwitchC-Ten-GigabitEthernet1/0/2] qos priority 6
   [SwitchC-Ten-GigabitEthernet1/0/2] quit
   ```

   # Assign port Ten-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 Ten-GigabitEthernet 1/0/3
   [SwitchC-Ten-GigabitEthernet1/0/3] port access vlan 20
   [SwitchC-Ten-GigabitEthernet1/0/3] qos priority 4
   [SwitchC-Ten-GigabitEthernet1/0/3] quit
   ```

   # Because the 802.1p priorities are carried in VLAN tags, you must configure Ten-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 Ten-GigabitEthernet 1/0/1
   [SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
   [SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 20
   [SwitchC-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   [SwitchC-Ten-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 Ten-GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 10 and 20.

```
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

Remove the port from VLAN 1.

```
[SwitchB-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure port Ten-GigabitEthernet 1/0/1 to trust the 802.1p priorities of received packets. 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.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Assign port Ten-GigabitEthernet 1/0/10 to VLAN 40.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/10
[SwitchB-Ten-GigabitEthernet1/0/10] port access vlan 40
```

Assign port Ten-GigabitEthernet 1/0/20 to VLAN 30.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/20
[SwitchB-Ten-GigabitEthernet1/0/20] port access vlan 30
```

Create VLAN interfaces and configure routing protocols to enable communication between network segments. For more information about these configurations, see *OSPF Configuration Examples*.

Enable byte-count WRR on egress port Ten-GigabitEthernet 1/0/20. By default, byte-count WRR is enabled.

```
[SwitchB-GigabitEthernet1/0/20] qos wrr byte-count
```

Configure the weight of queue 6 as twice that of queue 4. In this example, set the weight value to 4 for queue 6 and 2 for queue 4.

```
[SwitchB-Ten-GigabitEthernet1/0/20] qos wrr 4 group 1 byte-count 2
[SwitchB-Ten-GigabitEthernet1/0/20] qos wrr 6 group 1 byte-count 4
[SwitchB-Ten-GigabitEthernet1/0/20] quit
```

Configuring transmission priorities for the traffic to the Internet

1. Configure Switch B:

   # Enable SP queuing on port Ten-GigabitEthernet 1/0/10.

   ```
   [SwitchB] interface Ten-GigabitEthernet 1/0/10
   [SwitchB-Ten-GigabitEthernet1/0/10] qos sp
   ```

2. Configure Switch A:

   # Configure port Ten-GigabitEthernet 1/0/1 to trust the DSCP values of received packets.

   ```
   [SwitchA] interface Ten-GigabitEthernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] qos trust dscp
   ```

Modify the DSCP-to-802.1p priority mapping table to map DSCP value 33 to 802.1p priority 5 (queue 5).

```
[SwitchA] qos map-table dscp-dot1p
[SwitchA-maptbl-dscp-dot1p] import 33 export 5
[SwitchA-maptbl-dscp-dot1p] quit
```

The configuration assigns the three types of packets (HTTP, FTP, and Email) to queues 5, 4, and 3, respectively.

Enable byte-count WRR on Ten-GigabitEthernet 1/0/2. By default, byte-count WRR is enabled.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr byte-count
```

Set the weights of the three queues in the ratio of 2:1:1 (6, 3, and 3 in this example).

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr 5 group 1 byte-count 6
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr 4 group 1 byte-count 3
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr 3 group 1 byte-count 3
```

Configuration files

- Switch A:

```
#
qos map-table dscp-dot1p
 import 33 export 5
#
interface Ten-GigabitEthernet1/0/1
 qos trust dscp
#
interface Ten-GigabitEthernet1/0/2
 qos wrr byte-count
 qos wrr af3 group 1 byte-count 3
 qos wrr af4 group 1 byte-count 3
 qos wrr ef group 1 byte-count 6
```

- Switch B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/10
```

```
 port access vlan 40
#
interface Ten-GigabitEthernet1/0/20
 port access vlan 30
 qos wrr byte-count
 qos wrr af4 group 1 byte-count 2
 qos wrr cs6 group 1 byte-count 4
```

- Switch C:

```
#
vlan 10
#
vlan 20
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 10
 qos priority 6
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 20
 qos priority 4
```

Example: Configuring priority marking and queue scheduling

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

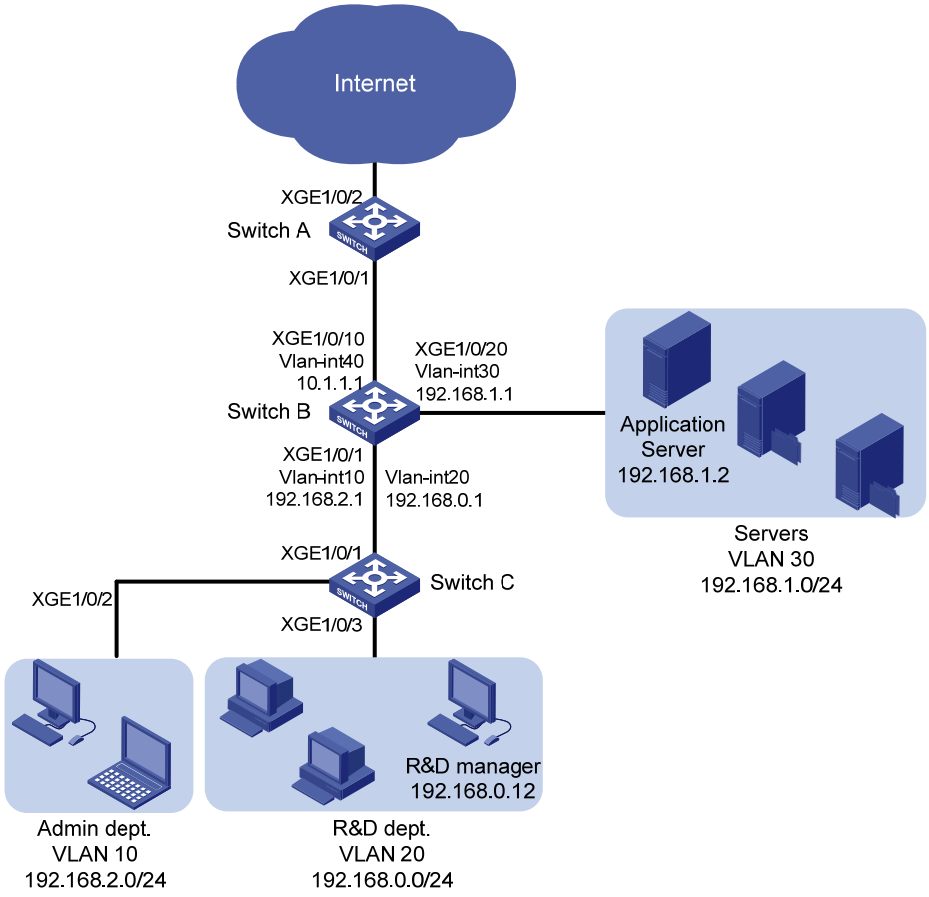
Network requirements

The network diagram of a company is shown in Figure 174. Configure priority marking and queue scheduling to meet the following requirements:

- **Access to the internal server farm**—The traffic from the Administration department takes priority over the traffic 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 the traffic 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. The three types of traffic is transmitted 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 174 Network diagram



Requirements analysis

Priority configuration for the internal network traffic

To meet the network requirements, you must perform the following tasks:

- 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, perform the following priority marking configurations:
  - Configure a class to match the traffic destined to the application server.

    - Configure a local precedence marking action for the class of traffic, so that all traffic that accesses the application server can be assigned to one queue.
    - Configure SP + WRR queuing on the egress port to preferentially transmit the traffic that accesses the application server.
- 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**.

Priority configuration for the Internet traffic

To meet the network requirements, you must perform the following tasks:

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.

As a result of the configurations, the traffic from the R&D department manager can be assigned the same local precedence value as the traffic from the Administration department.

For the email traffic from the Administration department, 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.

To assign packets with DSCP value 33 to a higher-priority queue, modify the DSCP-to-802.1p priority mapping table to map DSCP value 33 to a higher 802.1p priority value than the default. 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 by default.

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 Ten-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 Ten-GigabitEthernet 1/0/2
   [SwitchC-Ten-GigabitEthernet1/0/2] port access vlan 10
   [SwitchC-Ten-GigabitEthernet1/0/2] qos priority 6
   [SwitchC-Ten-GigabitEthernet1/0/2] quit
   ```

   # Assign port Ten-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 Ten-GigabitEthernet 1/0/3
   ```

```
[SwitchC-Ten-GigabitEthernet1/0/3] port access vlan 20
[SwitchC-Ten-GigabitEthernet1/0/3] qos priority 4
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, assign the port to VLAN 10 and VLAN 20, and remove the port from VLAN 1.

```
[SwitchC] interface Ten-GigabitEthernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[SwitchC-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchC-Ten-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 Ten-GigabitEthernet 1/0/1 as a trunk port.

```
<SwitchB> system-view
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 10 and 20.

```
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

Remove the port from VLAN 1.

```
[SwitchB-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure port Ten-GigabitEthernet 1/0/1 to trust the 802.1p priorities of received packets. 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.

```
[SwitchB-Ten-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Assign port Ten-GigabitEthernet 1/0/10 to VLAN 40.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/10
[SwitchB-Ten-GigabitEthernet1/0/10] port access vlan 40
```

Assign port Ten-GigabitEthernet 1/0/20 to VLAN 30.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/20
[SwitchB-Ten-GigabitEthernet1/0/20] port access vlan 30
```

Create VLAN interfaces and configure routing protocols to enable communication between network segments. For more information about these configurations, see *OSPF Configuration Examples*.

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 Ten-GigabitEthernet 1/0/1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] qos apply policy app_server inbound
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Enable byte-count WRR on Ten-GigabitEthernet 1/0/20. By default, byte-count WRR is enabled.

```
[SwitchB-Ten-GigabitEthernet1/0/20] qos wrr byte-count
```

Configure queue 7 as an SP queue on egress port Ten-GigabitEthernet 1/0/20.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/20
[SwitchB-Ten-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 that of queue 4. In this example, set the weight value to 4 for queue 6 and 2 for queue 4.

```
[SwitchB-Ten-GigabitEthernet1/0/20] qos wrr 6 group 1 byte-count 4
[SwitchB-Ten-GigabitEthernet1/0/20] qos wrr 4 group 1 byte-count 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 Ten-GigabitEthernet 1/0/3.

```
[SwitchC] interface Ten-GigabitEthernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] qos apply policy rd_manager inbound
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

2. Configure Switch B:

Enable SP queuing on port Ten-GigabitEthernet 1/0/10.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/10
[SwitchB-Ten-GigabitEthernet1/0/10] qos sp
```

3. Configure Switch A:

Configure port Ten-GigabitEthernet 1/0/1 to trust the DSCP values of received packets.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dscp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Modify the DSCP-to-802.1p priority mapping table to map DSCP value 33 to 802.1p priority 5 (queue 5).

```
[SwitchA] qos map-table dscp-dot1p
[SwitchA-maptbl-dscp-dot1p] import 33 export 5
[SwitchA-maptbl-dscp-dot1p] quit
```

The configuration assigns the three types of packets (HTTP, FTP, and Email) to queues 5, 4, and 3, respectively.

Enable byte-count WRR on Ten-GigabitEthernet 1/0/2. By default, byte-count WRR is enabled.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr byte-count
```

Set the weights for the three queues in the ratio of 2:1:1 (6, 3, and 3 in this example).

```
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr 5 group 1 byte-count 6
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr 4 group 1 byte-count 3
[SwitchA-Ten-GigabitEthernet1/0/2] qos wrr 3 group 1 byte-count 3
[SwitchA-Ten-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 Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy admin_email inbound
[SwitchA-Ten-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 Ten-GigabitEthernet1/0/1
 qos apply policy admin_email inbound
 qos trust dscp
#
interface Ten-GigabitEthernet1/0/2
 qos wrr byte-count
 qos wrr af3 group 1 byte-count 3
 qos wrr af4 group 1 byte-count 3
 qos wrr ef group 1 byte-count 6
```

- 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 Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 qos apply policy app_server inbound
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/10
 port access vlan 40
#
interface Ten-GigabitEthernet1/0/20
 port access vlan 30
 qos wrr byte-count
 qos wrr af4 group 1 byte-count 2
 qos wrr cs6 group 1 byte-count 4
 qos wrr cs7 group sp
```

- 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 Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 10
 qos priority 6
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 20
 qos apply policy rd_manager inbound
 qos priority 4
```

Configuration examples for implementing HQoS through marking local QoS IDs

This chapter provides examples for implementing HQoS through marking local QoS IDs.

Example: Configuring HQoS through marking local QoS IDs

Applicable product matrix

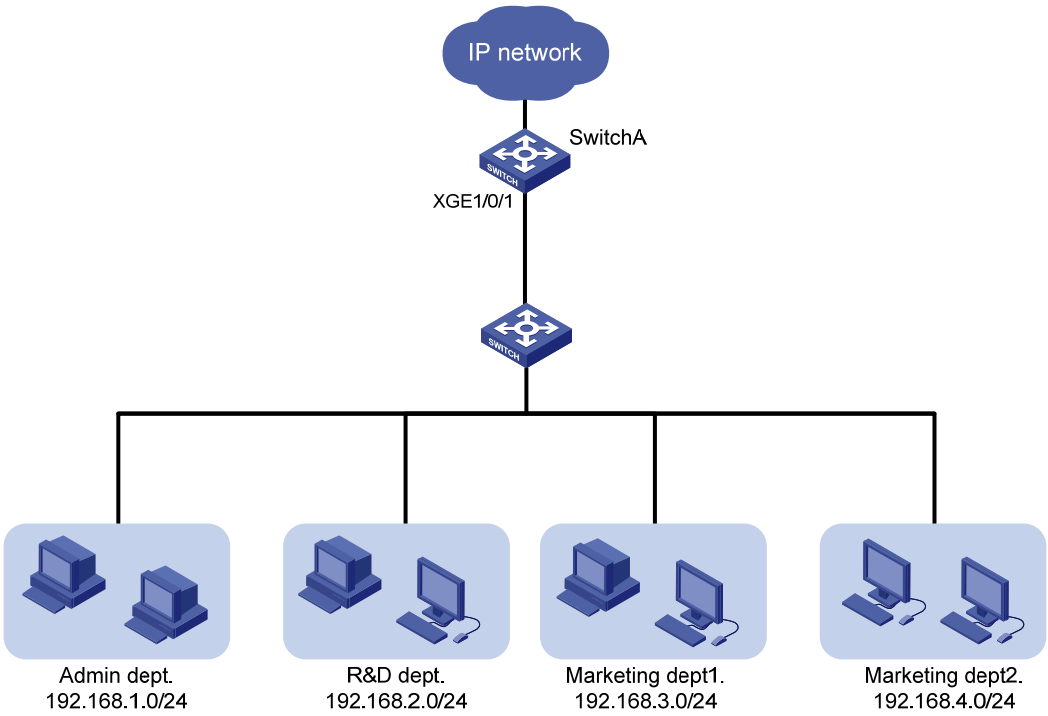
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 175, configure traffic policing and local QoS ID marking to limit the rate of traffic that accesses the IP network to meet the following requirements:

- 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 175 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 Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy car inbound
```

Verifying the configuration

Display information about QoS policies applied to Ten-GigabitEthernet 1/0/1.

```
[SwitchA] display qos policy interface Ten-GigabitEthernet 1/0/1
Interface: Ten-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 (Bytes), EBS 512 (Bytes)
        Green action: pass
        Yellow action: pass
        Red action: discard
        Green packets: 0 (Packets)
        Red packets: 0 (Packets)
   Classifier: rd
     Operator: AND
     Rule(s) : If-match acl 2002
     Behavior: car_admin_rd
      Committed Access Rate:
        CIR 1024 (kbps), CBS 64000 (Bytes), EBS 512 (Bytes)
        Green action: pass
        Yellow action: pass
        Red action: discard
        Green packets: 0 (Packets)
        Red packets: 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 (Bytes), EBS 512 (Bytes)
        Green action: pass
        Yellow action: pass
        Red action: discard
        Green packets: 0 (Packets)
        Red packets: 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 Ten-GigabitEthernet1/0/1
 qos apply policy car inbound
```

RBAC-based login user privilege configuration examples

Introduction

This chapter provides role based access control (RBAC) configuration examples to control access permissions of login users.

Assigning permissions to a user role includes the following:

- Define a set of rules to specify commands accessible or inaccessible to the user role.
- Configure resource access policies to specify which interfaces, VLANs, and VPN instances are accessible to the user role.

In this chapter, RBAC configuration examples are divided into the following types:

- Assign predefined user roles to login users (see Table 22).
- Assign user-defined user roles to login users (see Table 23).

  User-defined user roles are more flexible. You can configure user role rules and resource access policies in the user role to meet specific network requirements.

Table 22 Assigning predefined user roles to login users

Examples	Remarks
Example: Assigning predefined user role network-admin to login users	Predefined user roles include network-admin, network-operator, level-*n* (where *n* equals an integer in the range of 0 to 15), and security-audit. The network-admin, network-operator, level-15, or security-audit users cannot modify their own permissions. Level-0 to level-14 users can modify their own permissions for any commands except for the **display history-command all** command.

Table 23 Assigning user-defined user roles to login users

Configuration example subtype	Examples
Configure command rules	Example: Configuring login users to have access to specific commands
Configure feature rules	• Example: Configuring login users to have access to specific features • Example: Configuring login users to have access to specific command type of specific features • Example: Configuring login users to have access to specific commands of specific features • Example: Configuring login users to have access to ACL and QoS features

Configuration example subtype	Examples
Configure feature group rules	• Example: Configuring login users to have access to write commands of multiple features • Example: Configuring login users to have access to commands of predefined feature groups • Example: Configuring login users to have access to specific commands of a feature group
Configure user role interface policy	Example: Configuring login users to have access to specific commands on specific interfaces
Configure user role VLAN policy	Example: Configuring login users to have access to specific feature groups in specific VLANs
Configure user role VPN instance policy	Example: Configuring login users to have access to specific features in specific VPN instances
Assign multiple user roles to a user	• Example: Assigning another user role to change access permissions of a user • Example: Configuring login users to have access to ACL and QoS features
Configure temporary user role authorization	Example: Configuring temporary user role authorization

The login users obtain user roles only after they pass authentication. Table 24 shows the authentication modes for login users. For information about configuring authentication modes, see "Appendix Configuring authentication modes for login users."

Table 24 Authentication modes

Authentication mode	Remarks
none	Does not authenticate the username or password. Login users obtain the user roles on user interfaces.
password	Only authenticates the password. Login users obtain the user roles on user interfaces.
scheme	Authenticates both the username and password. • Local AAA—Login users obtain the user role in the local attributes. • Remote AAA—Login users obtain the user roles authorized by an AAA server. NOTE: In remote AAA authentication mode, an SSH login user who uses publickey or password-publickey authentication obtains the user roles specified in the view of the SSH user account.

NOTE:

Login users include SSH, Telnet, FTP, and terminal users who log in to the device. In this chapter, Telnet users are used.

Example: Assigning predefined user role network-admin to login users

Applicable product matrix

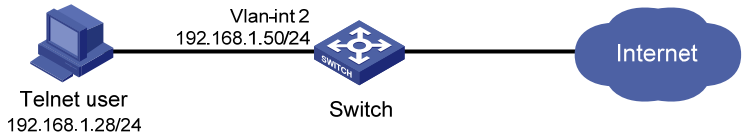
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 176, configure the switch to perform the following operations:

- Allow the Telnet user to log in without authentication.
- Assign the user role **network-admin** to the Telnet user.

Figure 176 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Configure the **none** authentication mode on VTY user interfaces, so the Telnet user (a VTY user) can log in to the switch without authentication. By default, the authentication mode is **password**.
- Assign the user role **network-admin** to VTY user interfaces, so the Telnet user can obtain this user role after it logs in to the switch.

Configuration procedures

Assign an IP address to VLAN-interface 2, as shown in Figure 176. Make sure the Telnet user and switch can reach each other. (Details not shown.)

Configure the **none** authentication mode on VTY user interfaces. For information about the configuration steps, see "Configuring none authentication mode for login users."

Assign user role **network-admin** to VTY user interfaces 0 to 15.

```
<Switch> system-view
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] user-role network-admin
```

```
[Switch-ui-vty0-15] quit
```

Verifying the configuration

1. Telnet to the switch. Verify that you can log in to the switch without authentication.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

2. Verify that you can execute RBAC commands. The user role **network-admin** has the access to RBAC feature.

   # Create user role **role1**.

```
<Switch> system-view
[Switch] role name role1
```

   # Deny the access of **role1** to any write commands of the **vlan** feature.

```
[Switch-role-role1] rule 1 deny write feature vlan
[Switch-role-role1] quit
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
```

Example: Configuring login users to have access to specific commands

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

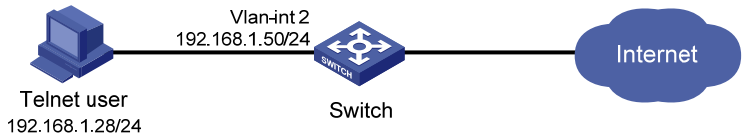
As shown in Figure 177, configure the switch to perform the following operations:

- Implement password authentication for VTY users, including the Telnet user at 192.168.1.28/24.
- Assign only the user role **role1** to the Telnet user.

Configure **role1** to have the following access permissions:

- Execute all commands that start with **display**.
- Create VLANs and execute all commands available in VLAN interface view.
- Deny the access to any VLANs except VLANs 10 to 20.
- Execute all commands available in interface view.
- Deny the access to any interfaces except Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/20 and VLAN-interfaces 10 to 16.

Figure 177 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Enable the **password** authentication mode and configure a password, so the switch can perform password authentication for VTY users, including the Telnet user.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, and VLANs.
- Remove the default user role after you assign **role1** to the VTY user interfaces, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure user role rules, follow these restrictions and guidelines:

- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 177. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure password authentication for the Telnet user.

   For information about the configuration steps, see "Configuring password authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands that start with **display**.

   ```
   [Switch-role-role1] rule 1 permit command display *
   ```

   # Configure rule 2 to permit the user role to create VLANs and execute all commands available in VLAN view.

   ```
   [Switch-role-role1] rule 2 permit command system-view ; vlan *
   ```

   # Configure rule 3 to permit the user role to execute all commands available in interface view.

   ```
   [Switch-role-role1] rule 3 permit command system-view ; interface *
   ```
4. Configure a VLAN policy for user role **role1**:

   # Enter user role VLAN policy view, and deny the user role to access any VLANs.

   ```
   [Switch-role-role1] vlan policy deny
   ```

   # Permit the user role to access VLANs 10 to 20.

   ```
   [Switch-role-role1-vlanpolicy] permit vlan 10 to 20
   [Switch-role-role1-vlanpolicy] quit
   ```
5. Configure an interface policy for user role **role1**:

   # Enter user role interface policy view, and deny the user role to access any interfaces.

   ```
   [Switch-role-role1] interface policy deny
   ```

   # Permit the user role to access Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/20.

   ```
   [Switch-role-role1-ifpolicy] permit interface ten-gigabitethernet 1/0/10 to
   ten-gigabitethernet 1/0/20
   ```

   # Permit the user role to access VLAN-interfaces 10 to 16.

   ```
   [Switch-role-role1-ifpolicy] permit interface vlan-interface 10 to vlan-interface 16
   ```

```
[Switch-role-role1-ifpolicy] quit
[Switch-role-role1] quit
```

6. Assign user role **role1** to VTY users:

   # Assign user role **role1** to user interfaces VTY 0 to 15.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] user-role role1
```

   # Remove the default user role **network-operator** from the VTY user interfaces.

```
[Switch-ui-vty0-15] undo user-role network-operator
[Switch-ui-vty0-15] quit
```

Verifying the configuration

1. Verify that the user role configuration is correct.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: deny
  Permitted VLANs: 10 to 20
  Interface policy: deny
  Permitted interfaces: Ten-GigabitEthernet1/0/10 to Ten-GigabitEthernet1/0/20,
Vlan-interface10 to Vlan-interface16
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit       command       display *
  2       permit       command       system-view ; vlan *
  3       permit       command       system-view ; interface *
  R:Read W:Write X:Execute
```

2. Telnet to the switch and enter the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Password:
<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute the read commands of all features. For example, use the **display clock** command to display date and time.

```
<Switch> display clock
09:31:56 UTC Tues 01/01/2013
<Switch>
```

   # Verify that you can access VLANs 10 to 20. For example, create VLAN 20.

```
<Switch> system-view
[Switch] vlan 20
[Switch-vlan20] quit
```

Verify that you cannot access other VLANs except VLANs 10 to 20. For example, create VLAN 30.

```
[Switch] vlan 30
Permission denied.
```

Verify that you can display information about all VLANs. For example, display information about VLANs 10 to 24.

```
[Switch] display vlan 10 to 24
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/10

VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:   None
 Untagged ports: None

 VLAN ID: 24
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0024
 Name: VLAN 0024
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/20
```

Verify that you can assign Ten-GigabitEthernet 1/0/10 (in VLAN 10) to VLAN 20.

```
[Switch] vlan 20
[Switch-vlan20] port ten-gigabitethernet 1/0/10
[Switch-vlan20] quit
```

Verify that you cannot assign Ten-GigabitEthernet 1/0/20 (in VLAN 24) to VLAN 20.

```
[Switch] vlan 20
[Switch-vlan20] port ten-gigabitethernet 1/0/20
Permission denied.
[Switch-vlan20] quit
```

Verify that you can access VLAN-interfaces 10 to 16. For example, enter the view of VLAN-interface 10.

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] quit
```

Verify that you cannot access other interfaces except Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/20 and VLAN-interfaces 10 to 16. For example, enter the view of VLAN-interface 20.

```
[Switch] interface vlan-interface 20
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 user-role role1
set authentication password hash $h$6$vaSj2xKc8yFiNdfQ$Jzb3PXo2ltTPcgyTQJZShe4j
kKSZqJUVhjP634Wol/Qx8TLU748IHoeui0w5n/XRzpNqbNnpxikym39gGJCwYw==
#
role name role1
 rule 1 permit command display *
 rule 2 permit command system-view ; vlan *
 rule 3 permit command system-view ; interface *
 vlan policy deny
  permit vlan 10 to 20
 interface policy deny
  permit interface Ten-GigabitEthernet1/0/10 to Ten-GigabitEthernet1/0/20
  permit interface Vlan-interface10 to Vlan-interface16
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific features

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

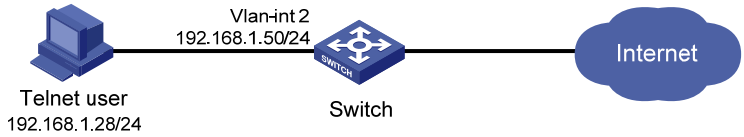
As shown in Figure 178, configure the switch to perform the following operations:

- Implement password authentication for VTY users, including the Telnet user at 192.168.1.28/24.
- Assign only the user role **role1** to the Telnet user.

Configure **role1** to have the following access permissions:

- Execute all commands of **aaa** and **device** features.
- Access all interfaces, VLANs, and VPN instances.

Figure 178 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Enable the **password** authentication mode and configure a password, so the switch can perform password authentication for login users, including the Telnet user.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, VLANs, and VPN instances. In this example, the user role has no access restrictions to interfaces, VLANs, and VPN instances, so you do not need to configure resource access policies.
- Remove the default user role after you assign **role1** to the VTY user interfaces, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure user role rules, follow these restrictions and guidelines:

- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 178. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure password authentication for the Telnet user.

   For information about the configuration steps, see "Configuring password authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands available for the **aaa** feature.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature aaa
   ```

   # Configure rule 2 to permit the user role to execute all commands available for the **device** feature.

   ```
   [Switch-role-role1] rule 2 permit execute read write feature device
   [Switch-role-role1] quit
   ```
4. Assign user role **role1** to VTY users:

   # Assign the user role to VTY user interfaces 0 to 15.

   ```
   [Switch] user-interface vty 0 15
   [Switch-ui-vty0-15] user-role role1
   ```

   # Remove the default user role **network-operator** from the VTY user interfaces.

   ```
   [Switch-ui-vty0-15] undo user-role network-operator
   [Switch-ui-vty0-15] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

   ```
   [Switch] display role name role1
   Role: role1
     Description:
     VLAN policy: permit (default)
     Interface policy: permit (default)
     VPN instance policy: permit (default)
     ----------------------------------------------------------------------
     Rule    Perm   Type  Scope         Entity
     ----------------------------------------------------------------------
     1       permit RWX   feature       aaa
   ```

```
  2       permit RWX   feature       device
  R:Read W:Write X:Execute
```

2. Telnet to the switch and enter the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Password:
<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute all commands of the **aaa** feature. For example, create domain **bbb** and enter ISP domain view.

```
<Switch> system-view
[Switch] domain bbb
[Switch-isp-bbb] quit
```

   # Verify that you can execute all commands of the **device** feature. For example, name the switch as **Switch-a**.

```
[Switch] sysname Switch-a
[Switch-a]
```

   # Verify that you cannot access commands of other features. For example, create VLAN 30.

```
[Switch-a] vlan 30
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 user-role role1
 set authentication password hash $h$6$vaSj2xKc8yFiNdfQ$Jzb3PXo2ltTPcgyTQJZShe4j
kKSZqJUVhjP634Wol/Qx8TLU748IHoeui0w5n/XRzpNqbNnpxikym39gGJCwYw==
#
role name role1
 rule 1 permit read write execute feature aaa
```

```
 rule 2 permit read write execute feature device
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific command type of specific features

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 179, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.
- Assign only the user role **role1** to the Telnet user.

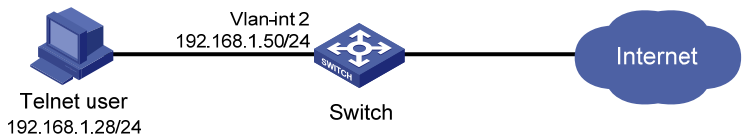
Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all write commands of the **device** feature.
- Execute all read and write commands of the **filesystem** feature.

Figure 179 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, VLANs, and VPN instances. In this example, the

user role has no access restrictions to interfaces, VLANs, and VPN instances, so you do not need to configure resource access policies.

- Remove the default user role after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 179. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration steps, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all write commands of the **device** feature.

   ```
   [Switch-role-role1] rule 1 permit write feature device
   ```

   # Configure rule 2 to permit the user role to execute all read and write commands of the **filesystem** feature.

   ```
   [Switch-role-role1] rule 2 permit read write feature filesystem
   [Switch-role-role1] quit
   ```
4. Assign user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user **telnetuser**.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Assign user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

   ```
   [Switch-luser-manage-telnetuser] undo authorization-attribute user-role
   network-operator
   [Switch-luser-manage-telnetuser] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------
  1       permit -W-   feature       device
  2       permit RW-   feature       filesystem
  R:Read W:Write X:Execute
```

2. Telnet to the switch, and enter the username **telnetuser@bbb** and the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute all write commands of the **device** feature. For example, name the switch as **Switch-a**.

```
<Switch> system-view
[Switch] sysname Switch-a
[Switch-a]
```

   # Verify that you cannot execute the read commands of the **device** feature. For example, use the **display clock** command to display date and time.

```
[Switch-a] display clock
Permission denied.
```

   # Verify that you can execute all read and write commands of the **filesystem** feature. For example, specify the source IPv4 address for outgoing FTP packets.

```
[Switch-a] ftp client source ip 192.168.0.60
[Switch-a] quit
```

   # Verify that you cannot use the execute commands of the **filesystem** feature. For example, log in to an FTP server and enter FTP client view.

```
<Switch-a> ftp
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit write feature device
 rule 2 permit read write feature filesystem
#
local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific commands of specific features

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 180, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.
- Assign only the user role **role1** to the Telnet user.

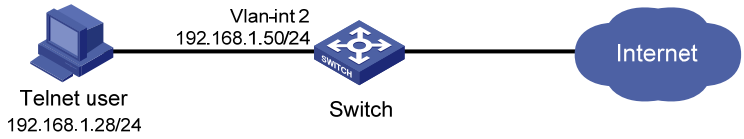
Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all read and write commands of the **device** feature.
- Deny all commands that start with **reboot**.

Figure 180 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, VLANs, and VPN instances. In this example, the user role has no access restrictions to interfaces, VLANs, and VPN instances, so you do not need to configure resource access policies.
- Remove the default user role after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 180. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration steps, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all read and write commands of the **device** feature.

   ```
   [Switch-role-role1] rule 1 permit read write feature device
   ```

   # Configure rule 2 to deny the user role to execute any commands that start with **reboot**.

   ```
   [Switch-role-role1] rule 2 deny command reboot *
   [Switch-role-role1] quit
   ```
4. Assign user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user **telnetuser**.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Assign user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

   ```
   [Switch-luser-manage-telnetuser] undo authorization-attribute user-role
   network-operator
   [Switch-luser-manage-telnetuser] quit
   ```

Verifying the configuration

1. Verify that the user role rule configuration is correct.

   ```
   [Switch] display role name role1
   Role: role1
     Description:
     VLAN policy: permit (default)
     Interface policy: permit (default)
     VPN instance policy: permit (default)
     ----------------------------------------------------------------------
     Rule    Perm   Type  Scope         Entity
     ----------------------------------------------------------------------
     1       permit RW-   feature       device
     2       deny         command       reboot *
     R:Read W:Write X:Execute
   ```
2. Telnet to the switch, and enter the username **telnetuser@bbb** and the password. Verify that you can log in to the switch.

   ```
   C:\Documents and Settings\user> telnet 192.168.1.50
   ```

```
**************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute the read commands of the **device** feature. For example, use the **display clock** command to display date and time.

   ```
   <Switch> display clock
   09:31:56 UTC Tues 01/01/2013
   <Switch>
   ```

   # Verify that you can execute the write commands of the **device** feature. For example, name the switch as **Switch-a**.

   ```
   <Switch> system-view
   [Switch] sysname Switch-a
   [Switch-a] quit
   ```

   # Verify that you cannot execute the commands that start with **reboot**.

   ```
   <Switch-a> reboot
   Permission denied.
   ```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
```

```
 rule 1 permit read write feature device
 rule 2 deny command reboot *
#
local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to write commands of multiple features

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 181, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.
- Assign only the user role **role1** to the Telnet user.

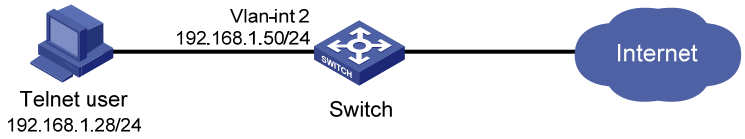
Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all write commands of the **aaa**, **device**, **interface**, **snmp**, **telnet**, and **vlan** features.
- Execute all commands that start with **display**.
- Deny the access to any VLANs except VLANs 10 to 20.
- Deny the access to any interfaces except Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/20 and VLAN-interfaces 10 to 16.

Figure 181 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, and VLANs.
- Assign the **aaa**, **device**, **interface**, **snmp**, **telnet**, and **vlan** features to a feature group and configure a feature group rule in user role **role1**, so the user role can access the write commands of these features.
- Remove the default user role after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 181. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration steps, see "Configuring local AAA authentication mode for login users."
3. Configure feature group **device-features**:

   # Create feature group **device-features**.

   ```
   <Switch> system-view
   [Switch] role feature-group name device-features
   ```

Add features **aaa**, **device**, **interface**, **snmp**, **telnet**, and **vlan** to the group.

```
[Switch-featuregrp-device-features] feature aaa
[Switch-featuregrp-device-features] feature device
[Switch-featuregrp-device-features] feature interface
[Switch-featuregrp-device-features] feature snmp
[Switch-featuregrp-device-features] feature telnet
[Switch-featuregrp-device-features] feature vlan
[Switch-featuregrp-device-features] quit
```

4. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all write commands of the feature group **device-features**.

   ```
   [Switch-role-role1] rule 1 permit write feature-group device-features
   ```

   # Configure rule 2 to permit the user role to execute all commands that start with **display**.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```

5. Configure a VLAN policy for user role **role1**:

   # Enter user role VLAN policy view, and deny the user role to access any VLANs.

   ```
   [Switch-role-role1] vlan policy deny
   ```

   # Permit the user role to access VLANs 10 to 20.

   ```
   [Switch-role-role1-vlanpolicy] permit vlan 10 to 20
   [Switch-role-role1-vlanpolicy] quit
   ```

6. Configure an interface policy for user role **role1**:

   # Enter user role interface policy view, and deny the user role to access any interfaces.

   ```
   [Switch-role-role1] interface policy deny
   ```

   # Permit the user role to access Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/20.

   ```
   [Switch-role-role1-ifpolicy] permit interface ten-gigabitethernet 1/0/10 to
   ten-gigabitethernet 1/0/20
   ```

   # Permit the user role to access VLAN-interfaces 10 to 16.

   ```
   [Switch-role-role1-ifpolicy] permit interface vlan-interface 10 to vlan-interface 16
   [Switch-role-role1-ifpolicy] quit
   [Switch-role-role1] quit
   ```

7. Assign user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user **telnetuser**.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Assign user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

   ```
   [Switch-luser-manage-telnetuser] undo authorization-attribute user-role
   network-operator
   [Switch-luser-manage-telnetuser] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: deny
  Permitted VLANs: 10 to 20
  Interface policy: deny
  Permitted interfaces: Ten-GigabitEthernet1/0/10 to Ten-GigabitEthernet1/0/20,
Vlan-interface10 to Vlan-interface16
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  1       permit -W-   feature-group device-features
  2       permit       command       display *
  R:Read W:Write X:Execute
```

2. Use the **display role feature-group** command to verify that the features have added to the feature group **device-features**.

```
[Switch] display role feature-group name device-features
Feature group: device-features
Feature: aaa             (AAA related commands)
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: snmp            (SNMP related commands)
Feature: telnet          (Telnet related commands)
Feature: vlan            (Virtual LAN related commands)
```

3. Telnet to the switch, and enter the username **telnetuser@bbb** and the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute the write commands of the **vlan** feature and access VLANs 10 to 20. For example, create VLAN 20.

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

   # Verify that you cannot access other VLANs except VLANs 10 to 20. For example, create VLAN 30.

```
[Switch] vlan 30
Permission denied.
```

Verify that you can display information about all VLANs. For example, display information about VLANs 10 to 24.

```
[Switch] display vlan 10 to 24
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/10

VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:   None
 Untagged ports: None

 VLAN ID: 24
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0024
 Name: VLAN 0024
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/20
```

Verify that you can assign Ten-GigabitEthernet 1/0/10 (in VLAN 10) to VLAN 20.

```
[Switch] vlan 20
[Switch-vlan20] port ten-gigabitethernet 1/0/10
# Verify that you cannot assign Ten-GigabitEthernet 1/0/20 (in VLAN 24) to VLAN 20.
[Switch-vlan20] port ten-gigabitethernet 1/0/20
Permission denied.
[Switch-vlan20] quit
```

Verify that you can execute the write commands of the **interface** feature and access VLAN-interfaces 10 to 16. For example, enter the view of VLAN-interface 10.

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] quit
[Switch] quit
```

Verify that you cannot use the execute commands of the **telnet** feature. For example, Telnet to a Telnet server.

```
<Switch> telnet 192.168.1.30
Permission denied.
```

Verify that you cannot use the execute commands of the **aaa** feature. For example, use the **super** command to obtain a temporary user role.

```
<Switch> super role2
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role feature-group name device-features
 feature aaa
 feature device
 feature interface
 feature snmp
 feature telnet
 feature vlan
#
role name role1
 rule 1 permit write feature-group device-features
 rule 2 permit command display *
 vlan policy deny
  permit vlan 10 to 20
 interface policy deny
  permit interface Ten-GigabitEthernet1/0/10 to Ten-GigabitEthernet1/0/20
  permit interface Vlan-interface10 to Vlan-interface16
#
local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to commands of predefined feature groups

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 182, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.
- Assign only the user role **role1** to the Telnet user.

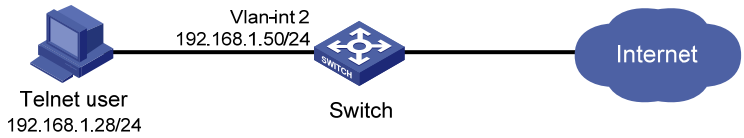
Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all commands of the predefined feature group **L2**.
- Execute all commands that start with **display**.
- Access all interfaces, VLANs, and VPN instances.

Figure 182 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, VLANs, and VPN instances. In this example, the user role has no access restrictions to interfaces, VLANs, and VPN instances, so you do not need to configure resource access policies.
- Remove the default user role from the user after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 182. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration steps, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands of the feature group **L2**.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L2
   ```

   # Configure rule 2 to permit the user role to execute all commands that start with **display**.

   ```
   [Switch-role-role1] rule 2 permit command display *
   [Switch-role-role1] quit
   ```
4. Assign user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user **telnetuser**.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Assign user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

   ```
   [Switch-luser-manage-telnetuser] undo authorization-attribute user-role
   network-operator
   [Switch-luser-manage-telnetuser] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

   ```
   [Switch] display role name role1
   Role: role1
   ```

```
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L2
  2       permit       command       display *
  R:Read W:Write X:Execute
```

2. Use the **display role feature-group** command to display the features in feature group **L2**. (Details not shown.)
3. Telnet to the switch, and enter the username **telnetuser@bbb** and the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute the commands of the **vlan** feature. For example, create VLAN 10 and assign Ten-GigabitEthernet 1/0/8 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port ten-gigabitethernet 1/0/8
[Switch-vlan10] quit
```

   # Verify that you can execute the commands that start with **display**. For example, use the **display clock** command to display date and time.

```
[Switch] display clock
09:31:56 UTC Tues 01/01/2013
[Switch] quit
```

   # Verify that you cannot use the execute commands of the **filesystem** feature. For example, log in to an FTP server and enter FTP client view.

```
<Switch> ftp
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
```

```
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L2
 rule 2 permit command display *
#
local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific commands of a feature group

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 183, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.

- Assign only the user role **role1** to the Telnet user.

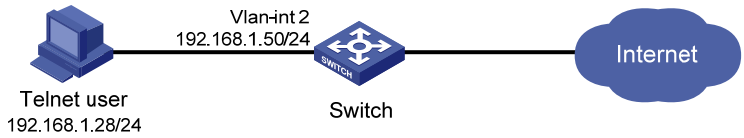
Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all commands of the predefined feature group **L3**.
- Execute all commands that start with **display**.
- Deny the access to read commands of the **vlan** feature.
- Access all interfaces, VLANs, and VPN instances.

Figure 183 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, VLANs, and VPN instances. In this example, the user role has no access restrictions to interfaces, VLANs, and VPN instances, so you do not need to configure resource access policies.
- Remove the default user role after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 183. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration steps, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands of the feature group **L3**.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L3
   ```

   # Configure rule 2 to permit the user role to execute all commands that start with **display**.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```

   # Configure rule 3 to deny the user role to execute any read commands of the **vlan** feature.

   ```
   [Switch-role-role1] rule 3 deny read feature vlan
   [Switch-role-role1] quit
   ```
4. Assign user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user **telnetuser**.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Assign user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

   ```
   [Switch-luser-manage-telnetuser] undo authorization-attribute user-role
   network-operator
   [Switch-luser-manage-telnetuser] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

   ```
   [Switch] display role name role1
   Role: role1
     Description:
     VLAN policy: permit (default)
     Interface policy: permit (default)
     VPN instance policy: permit (default)
     ----------------------------------------------------------------------
     Rule    Perm   Type  Scope         Entity
     ----------------------------------------------------------------------
     1       permit RWX   feature-group L3
     2       permit       command       display *
     3       deny   R--   feature       vlan
     R:Read W:Write X:Execute
   ```

2. Use the **display role feature-group** command to display the features in the feature group **L3**. (Details not shown.)
3. Telnet to the switch, and enter the username **telnetuser@bbb** and the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can use the write and execute commands of the **vlan** feature. For example, create VLAN 10 and assign Ten-GigabitEthernet 1/0/8 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port ten-gigabitethernet 1/0/8
[Switch-vlan10] quit
```

   # Verify that you can execute all commands that start with **display**, except for the **display** commands of the **vlan** feature. For example, use the **display clock** command to display date and time.

```
[Switch] display clock
09:31:56 UTC Tues 01/01/2013
[Switch]
```

   # Verify that you cannot use any read commands of the **vlan** feature. For example, use the **display vlan** command.

```
[Switch] display vlan
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
```

```
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 rule 3 deny read feature vlan
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific commands on specific interfaces

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 184, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.
- Assign only the user role **role1** to the Telnet user.

Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

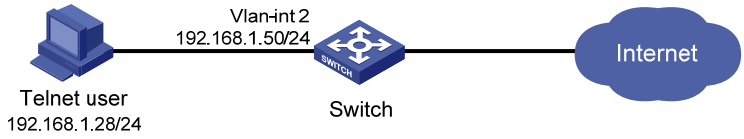
Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all commands that start with **display**.

- Create VLANs and assign ports to VLANs.
- Enter Ethernet interface view.
- Enter VLAN interface view and execute all commands available in VLAN interface view.
- Deny the access to any interfaces except Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/24 and VLAN-interface 20.

Figure 184 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands and interfaces.
- Remove the default user role after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 184. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration steps, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

```
<Switch> system-view
[Switch] role name role1
```

Configure rule 1 to permit the user role to execute all commands that start with **display**.

```
[Switch-role-role1] rule 1 permit command display *
```

Configure rule 2 to permit the user role to create VLANs and assign ports to VLANs.

```
[Switch-role-role1] rule 2 permit command system; vlan *; port *
```

Configure rule 3 to permit the user role to access the views of Ten-GigabitEthernet interfaces.

```
[Switch-role-role1] rule 3 permit command system; interface Ten-GigabitEthernet *;
```

Configure rule 4 to permit the user role to execute all commands available in VLAN interface view.

```
[Switch-role-role1] rule 4 permit command system; interface Vlan-interface *
```

4. Configure an interface policy for user role **role1**:

Enter user role interface policy view, and deny the user role to access any interfaces.

```
[Switch-role-role1] interface policy deny
```

Permit the user role to access Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/24.

```
[Switch-role-role1-ifpolicy] permit interface ten-gigabitethernet 1/0/1 to
ten-gigabitethernet 1/0/24
```

Permit the user role to access VLAN-interface 20.

```
[Switch-role-role1-ifpolicy] permit interface vlan-interface 20
[Switch-role-role1-ifpolicy] quit
[Switch-role-role1] quit
```

5. Assign user role **role1** to device management user **telnetuser**:

Enter the view of the device management user **telnetuser**.

```
[Switch] local-user telnetuser class manage
```

Assign user role **role1** to the user.

```
[Switch-luser-manage-telnetuser] authorization-attribute user-role role1
```

Remove the default user role **network-operator** from the user.

```
[Switch-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnetuser] quit
```

Verifying the configuration

1. Verify that the user role configuration is correct.

```
[Switch] display role name role1
Role: role1
Description:
  VLAN policy: permit (default)
  Interface policy: deny
  Permitted interfaces: Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/24, V
lan-interface20
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit       command       system; vlan *; port *
```

```
  2       permit       command       display *
  3       permit       command       system; interface Ten-GigabitEth
                                     ernet *;
  4       permit       command       system; interface Vlan-interface
                                      *
  R:Read W:Write X:Execute
```

2. Use the **display role feature-group** command to display the features in feature group **L3**. (Details not shown.)
3. Telnet to the switch, and enter the username **telnetuser@bbb** and the configured password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can create VLANs and assign ports to VLANs. For example, create VLAN 20 and assign Ten-GigabitEthernet 1/0/8 to VLAN 20.

```
<Switch> system-view
[Switch] vlan 20
[Switch-vlan20] port ten-gigabitethernet 1/0/8
```

   # Verify that you cannot assign other ports to VLAN 20 except Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/24. For example, assign Ten-GigabitEthernet 1/0/25 to VLAN 20.

```
[Switch-vlan20] port ten-gigabitethernet 1/0/25
Permission denied.
[Switch-vlan20] quit
```

   # Verify that you can execute the commands that start with **display** in interface view. For example, display the running configuration on Ten-GigabitEthernet 1/0/8.

```
[Switch] interface ten-gigabitethernet 1/0/8
[Switch-Ten-GigabitEthernet1/0/8] display this
#
interface Ten-GigabitEthernet1/0/8
 port access vlan 20
#
return
[Switch-Ten-GigabitEthernet1/0/8]
```

   # Verify that you cannot execute any commands in interface view, except for the **display**, **quit**, and **return** commands. For example, use the **shutdown** command to shut down a port.

```
[Switch-Ten-GigabitEthernet1/0/8] shutdown
Permission denied.
[Switch-Ten-GigabitEthernet1/0/8] quit
```

Verify that you can execute all commands available in VLAN interface view. For example, use the **vrrp vrid** command to create IPv4 VRRP group 1 on VLAN-interface 20 and assign virtual IP address 10.2.2.2 to the VRRP group.

```
[Switch] interface Vlan-interface 20
[Switch-Vlan-interface20] vrrp vrid 1 virtual-ip 10.2.2.2
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit command system; vlan *; port *
 rule 2 permit command display *
 rule 3 permit command system; interface Ten-GigabitEthernet *;
 rule 4 permit command system; interface Vlan-interface *
 interface policy deny
  permit interface Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/24
  permit interface Vlan-interface20
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific feature groups in specific VLANs

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 185, configure the switch to perform the following operations:

- Implement local authentication and authorization for the Telnet user.
- Assign only the user role **role1** to the Telnet user.

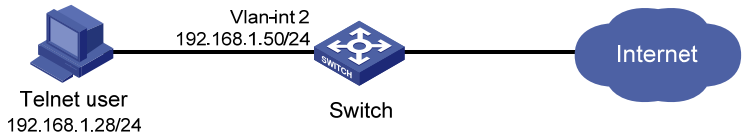
Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add device management user **telnetuser** and specify a password for the user. The Telnet user must use username **telnetuser@bbb** and the password to log in to the switch.

Configure **role1** to have the following permissions:

- Execute all commands available for the features in feature group **L2**.
- Execute all commands that start with **display**.
- Deny the access to any VLANs except VLANs 10 to 20.
- Deny the access to any interfaces except Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/20.

Figure 185 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands, interfaces, and VLANs.
- Remove the default user role after you assign **role1** to the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

When you configure local authentication and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the rule change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 185. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration procedure, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands available for the feature group **L2**.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L2
   ```

   # Configure rule 2 to permit the user role to execute the commands that starts with **display**.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```
4. Configure a VLAN policy for the user role **role1**:

   # Enter user role VLAN policy view, and deny the user role to access any VLANs.

   ```
   [Switch-role-role1] vlan policy deny
   ```

   # Permit the user role to access VLANs 10 to 20.

   ```
   [Switch-role-role1-vlanpolicy] permit vlan 10 to 20
   [Switch-role-role1-vlanpolicy] quit
   ```
5. Configure an interface policy for the user role **role1**:

   # Enter user role interface policy view, and deny the user role to access any interfaces.

   ```
   [Switch-role-role1] interface policy deny
   ```

   # Permit the user role to access Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/24.

   ```
   [Switch-role-role1-ifpolicy] permit interface ten-gigabitethernet 1/0/1 to
   ten-gigabitethernet 1/0/24
   [Switch-role-role1-ifpolicy] quit
   [Switch-role-role1] quit
   ```

6. Assign user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Assign user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

   ```
   [Switch-luser-manage-telnetuser] undo authorization-attribute user-role
   network-operator
   [Switch-luser-manage-telnetuser] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

   ```
   [Switch] display role name role1
   Role: role1
     Description:
     VLAN policy: deny
     Permitted VLANs: 10 to 20
     Interface policy: deny
     Permitted interfaces: Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/24
     VPN instance policy: permit (default)
     ----------------------------------------------------------------------
     Rule    Perm   Type  Scope         Entity
     ----------------------------------------------------------------------
     1       permit RWX   feature-group L2
     2       permit       command       display *
     R:Read W:Write X:Execute
   ```

2. Use the **display role feature-group** command to display the features in feature group **L2**. (Details not shown.)
3. Telnet to the switch, and enter the username **telnetuser@bbb** and the password. Verify that you can log in to the switch.

   ```
   C:\Documents and Settings\user> telnet 192.168.1.50

   ******************************************************************************
   * Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
   * Without the owner's prior written consent,                                 *
   * no decompiling or reverse-engineering shall be allowed.                    *
   ******************************************************************************

   login: telnetuser@bbb
   Password:
   <Switch>
   ```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute all commands available for the features in feature group **L2**. For example, create VLAN 20 and name the VLAN as **test**.

   ```
   <Switch> system-view
   [Switch] vlan 20
   ```

```
[Switch-vlan20] name test
[Switch-vlan20] display this
#
vlan 20
 name test
#
return
[Switch-vlan20] quit
```

Verify that you can enter Ethernet interface view. For example, enter the view of Ten-GigabitEthernet 1/0/8.

```
[Switch] interface ten-gigabitethernet 1/0/8
[Switch-Ten-GigabitEthernet1/0/8] quit
```

Verify that you cannot enter VLAN interface view. For example, enter the view of VLAN-interface 20.

```
[Switch] interface vlan-interface 20
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L2
 rule 2 permit command display *
 vlan policy deny
  permit vlan 10 to 20
 interface policy deny
  permit interface Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/24
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
```

```
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to specific features in specific VPN instances

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 186, configure the switch to perform the following operations:

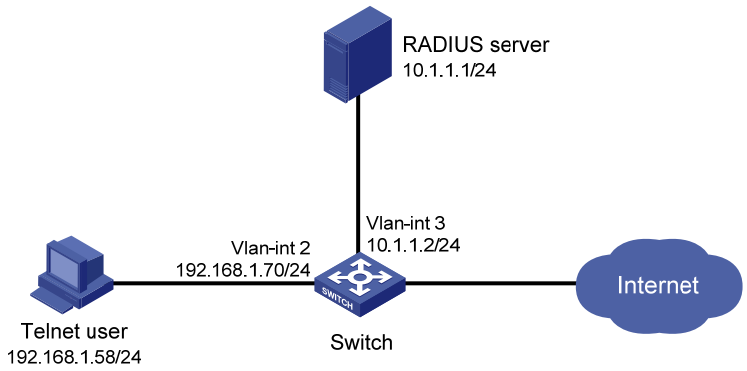
- Use the FreeRADIUS server at 10.1.1.1/24 for authentication and authorization of login users, including the Telnet user at 192.168.1.58/24.
- Use the shared key **aabbcc** for secure RADIUS communication between the switch and the server.
- Send usernames with their domain names to the server.
- Assign the user role **role1** to the Telnet user after the user passes authentication.

Create ISP domain **bbb**, in which the Telnet user is authenticated. The Telnet user must use the username **hello@bbb** to log in to the switch.

Configure **role1** to have the following access permissions:

- Execute all commands available for the features in feature group **L3**.
- Execute all commands that start with **display**.
- Deny the access to any VPN instances except **vpn1**, **vpn2**, and **vpn3**.

Figure 186 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Create user role **role1**, and configure user role rules and resource access policies for allowing the user role to access specific commands and VPN instances.
- Specify user role **role1** on the RADIUS server for the Telnet user, so the switch assigns this user role to the Telnet user after it passes authentication.

Configuration restrictions and guidelines

When you configure the remote AAA authentication mode and user role rules, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- RADIUS user authorization information is piggybacked in authentication responses. Use the same RADIUS scheme for user authentication and authorization.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Configuration procedures

1. Assign IP addresses to interfaces, as shown in Figure 186. Make sure the Telnet user, switch, and RADIUS server can reach each other. (Details not shown.)
2. Configure the remote AAA authentication mode for the Telnet user.

For information about the configuration procedure, see "Configure remote AAA authentication mode for login users."

3. Create user role **role1** and configure access permissions for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands available for the features in feature group **L3**.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L3
   ```

   # Configure rule 2 to permit the user role to execute all commands that start with **display**.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```

   # Enter user role VPN instance policy view, and deny the user role to access any VPN instances.

   ```
   [Switch-role-role1] vpn policy deny
   ```

   # Permit the user role to access VPN instances **vpn1**, **vpn2**, and **vpn3**.

   ```
   [Switch-role-role1-vpnpolicy] permit vpn-instance vpn1 vpn2 vpn3
   [Switch-role-role1-vpnpolicy] quit
   [Switch-role-role1] quit
   ```

4. Configure the RADIUS server:

   # Add the NAS IP address and shared key configuration to the **clients.conf** configuration file.

   ```
   client 10.1.1.2/24 {
     secret   = aabbcc
   ```

   # Add the Telnet user configuration to the **users** file.

   ```
   hello@bbb
     Cleartext-Password := "hello"
     Service-Type = Login-User,
     Login-Service = Telnet,
     Cisco-AVPair = "shell:roles=\"role1\""
   ```

   For more information about the server configuration, see the configuration guide for the server.

Verifying the configuration

1. Verify that the user role configuration is correct.

   ```
   [Switch] display role name role1
   Role: role1
     Description:
     VLAN policy: permit (default)
     Interface policy: permit (default)
     VPN instance policy: deny
     Permitted VPN instances: vpn1, vpn2, vpn3
     ------------------------------------------------------------------
     Rule    Perm   Type  Scope         Entity
     ------------------------------------------------------------------
     1       permit RWX   feature-group L3
     2       permit       command       display *
     R:Read W:Write X:Execute
   ```

2. Use the **display role feature-group** command to identify the features in feature group L3. (Details not shown.)
3. Telnet to the switch, and enter the username **hello@bbb** and the user's password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.70

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: hello@bbb
Password:
<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute the commands available for the features in feature group **L3**. For example, create VPN instance **vpn1** and configure an RD for the VPN instance.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] route-distinguisher 22:1
[Switch-vpn-instance-vpn1] display this
#
ip vpn-instance vpn1
 route-distinguisher 22:1
#
return
[Switch-vpn-instance-vpn1] quit
```

   # Verify that you cannot access any other VPN instances except **vpn1**, **vpn2**, and **vpn3**. For example, create VPN instance **vpn5**.

```
[Switch] ip vpn-instance vpn5
Permission denied.
```

Configuration files

```
#
 telnet server enable
#

vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.70 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
```

```
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZIcJhzscTHLA4WasBVh0UOw==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 vpn-instance policy deny
  permit vpn-instance vpn1
  permit vpn-instance vpn2
  permit vpn-instance vpn3
#
```

Example: Assigning another user role to change access permissions of a user

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 187:

- The switch performs local authentication and authorization for Telnet users.
- The Telnet users must be authenticated in ISP domain **bbb**.
- The Telnet users are assigned the user role **role1** after they pass authentication.

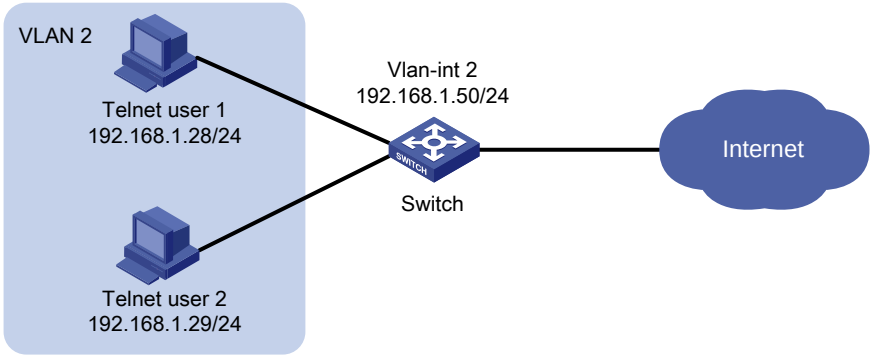
User role **role1** has the following access permissions:

- Execute all commands that start with **display**.
- Create VLANs and execute commands available in VLAN view.
- Deny the access to any VLANs except VLANs 10 to 15.
- Deny the access to any interfaces except Ten-GigabitEthernet 1/0/10 to Ten-GigabitEthernet 1/0/15.

Besides the permissions of user role **role1**, add the following access permissions to Telnet user **telnetuser1**:

- Enter VLAN interface view and execute commands available in VLAN interface view.
- Access VLANs 16 to 20.
- Access Ten-GigabitEthernet 1/0/16 to Ten-GigabitEthernet 1/0/20 and VLAN-interfaces 16 to 20.

Figure 187 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the users can Telnet to the switch. By default, the Telnet server function is disabled.
- Assign another user role to **telnetuser1** for adding access permissions to the user:
  a. Create a new user role named **role2**.
  b. Add the required access permissions to user role **role2**.
  c. Assign user role **role2** to **telnetuser1** in local user view.

Configuration restrictions and guidelines

When you assign multiple user roles to a user, follow these restrictions and guidelines:

- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping**

command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

- If multiple user roles are assigned to a user, the user can use the collection of commands and resources accessible to all the user roles.
- The newly-assigned user role does not take effect at the current login.

Configuration procedures

1. Create user role **role2** and configure rules for the user role:

   # Create user role **role2** and enter its view.

   ```
   <Switch> system-view
   [Switch] role name role2
   ```

   # Configure rule 1 to permit the user role to access VLAN interface view, and to execute all commands available in VLAN interface view.

   ```
   [Switch-role-role2] rule 1 permit command system-view ; interface vlan-interface *
   ```

2. Configure a VLAN policy for user role **role2**:

   # Enter user role VLAN policy view, and deny the user role to access any VLANs.

   ```
   [Switch-role-role2] vlan policy deny
   ```

   # Permit the user role to access VLANs 16 to 20.

   ```
   [Switch-role-role2-vlanpolicy] permit vlan 16 to 20
   [Switch-role-role2-vlanpolicy] quit
   ```

3. Configure an interface policy for user role **role2**:

   # Enter user role interface policy view, and deny the user role to access any interfaces.

   ```
   [Switch-role-role2] interface policy deny
   ```

   # Permit the user role to access Ten-GigabitEthernet 1/0/16 through Ten-GigabitEthernet 1/0/20.

   ```
   [Switch-role-role2-ifpolicy] permit interface ten-gigabitethernet 1/0/16 to
   ten-gigabitethernet 1/0/20
   ```

   # Permit the user role to access VLAN-interfaces 16 to 20.

   ```
   [Switch-role-role2-ifpolicy] permit interface vlan-interface 16 to vlan-interface 20
   [Switch-role-role2-ifpolicy] quit
   [Switch-role-role2] quit
   ```

4. Assign user role **role2** to device management user **telnetuser1**:

   # Enter the view of the device management user.

   ```
   [Switch] local-user telnetuser1 class manage
   ```

   # Assign user role **role2** to the user.

   ```
   [Switch-luser-manage-telnetuser1] authorization-attribute user-role role2
   [Switch-luser-manage-telnetuser1] quit
   ```

Verifying the configuration

1. Verify that the user role configuration is correct.

   ```
   [Switch] display role name role2
   Role: role2
     Description:
   ```

```
  VLAN policy: deny
  Permitted VLANs: 16 to 20
  Interface policy: deny
  Permitted interfaces: Ten-GigabitEthernet1/0/16 to Ten-GigabitEthernet1/0/20,
Vlan-interface16 to Vlan-interface20
  VPN instance policy: permit (default)
  -------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  -------------------------------------------------------------------
  1       permit       command       system-view ; interface vlan-int
                                     erface *
  R:Read W:Write X:Execute
```

2. Telnet to the switch, and enter the username **telnetuser1@bbb** and the user's password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser1@bbb
Password:
<Switch>
```

3. Verify that you have the access permissions of user roles **role1** and **role2**:

   # Verify that you can execute the commands that start with **display**. For example, use the **display vlan** command display information about VLANs 10 to 24.

```
<Switch> display vlan 10 to 24
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/10

VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:   None
 Untagged ports: None

 VLAN ID: 24
 VLAN type: Static
```

```
Route interface: Not configured
Description: VLAN 0024
Name: VLAN 0024
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/20
```

Verify that you can access VLANs 10 to 20 and execute commands in VLAN view. For example, assign Ten-GigabitEthernet 1/0/10 (in VLAN 10) to VLAN 20.

```
<Switch> system-view
[Switch] vlan 20
[Switch-vlan20] port ten-gigabitethernet 1/0/10
```

Verify that you cannot access any other VLANs except VLANs 10 to 20. For example, assign Ten-GigabitEthernet 1/0/20 (in VLAN 24) to VLAN 20.

```
[Switch-vlan20] port ten-gigabitethernet 1/0/20
Permission denied.
[Switch-vlan20] quit
```

Verify that you can enter VLAN interface view of VLANs 16 to 20 and execute commands available in VLAN interface view. For example, enter the view of VLAN-interface 20 and assign an IP address to the interface.

```
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] ip address 192.168.0.80 255.255.255.0
[Switch-Vlan-interface20] quit
```

Verify that you cannot access the views of Ethernet interfaces. For example, enter the view of Ten-GigabitEthernet 1/0/20.

```
[Switch] interface ten-gigabitethernet 1/0/20
Permission denied.
```

Verify that you cannot enter the view of other VLAN interfaces except VLAN-interfaces 16 to 20. For example, enter the view of VLAN-interface 15.

```
[Switch] interface vlan-interface 15
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
```

```
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit command display *
 rule 2 permit command system-view ; vlan *
 vlan policy deny
  permit vlan 10 to 15
 interface policy deny
  permit interface Ten-GigabitEthernet1/0/10 to Ten-GigabitEthernet1/0/15
#
role name role2
 rule 1 permit command system-view ; interface vlan-interface *
 vlan policy deny
  permit vlan 16 to 20
 interface policy deny
  permit interface Ten-GigabitEthernet1/0/16 to Ten-GigabitEthernet1/0/20
  permit interface Vlan-interface16 to Vlan-interface20
#
 local-user telnetuser1 class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
 authorization-attribute user-role role2
#
 local-user telnetuser2 class manage
 password hash TPcgyTQJZShe$h$6$vaSj2xKc8yFiNdfQ$Jzb3PXo2lt4jk KSZqJUVhjP634Wol/
Qx8TLU748IHoeui0w5n/XRzpNqbNnpxikym39gGJCwYw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring temporary user role authorization

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 188:

- The switch performs local authentication and authorization for login users, which include the Telnet user.
- The Telnet user is authenticated in ISP domain **bbb** and uses the username **telnetuser@bbb**.
- The Telnet user is assigned the user role **role1** after it passes authentication.

Configure local authentication for temporary user role authorization. The switch provides authentication for user roles **role1**, **role2**, and **network-operator**.

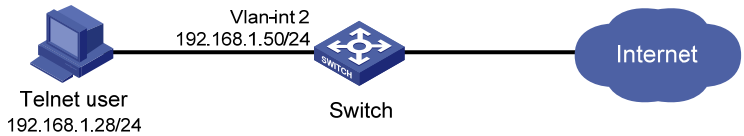
Configure **role1** to have the following permissions:

- Execute all commands available for the features in the predefined feature group **L3**.
- Execute all commands that start with **display**.
- Execute all commands that start with **super**.
- Access any interfaces, VLANs, and VPN instances.

Configure **role2** to have the following permissions:

- Execute all commands available for the features in the predefined feature group **L2**.
- Access any interfaces, VLANs, and VPN instances.

Figure 188 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Configure local authentication mode for temporary user role authorization, and configure a user role authentication password for security purposes.

Create user roles **role1** and **role2**, and configure user role rules and resource access policies for allowing the users to access specific commands, interfaces, VLANs, and VPN instances. In this example, the user roles have no access restrictions to interfaces, VLANs, and VPN instances, so you do not need to configure resource access policies.

- Remove the default user role from the user, so the switch assigns only the user role **role1** to the Telnet user.

Configuration restrictions and guidelines

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

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- If the rule with the specified ID does not exist, the **rule** command creates the user role rule. If the rule with the specified ID has existed, the **rule** command changes the user role rule.
- Any rule modification, addition, or removal for a user role takes effect only on users who log in with the user role after the change.
- A user role can access the set of permitted commands specified in its rules. If two rules of the same type conflict, the one with the higher ID takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.
- Temporary user role authorization is effective only on the current login. It does not change the user role settings in the user account that you have been logged in with. The next time you are logged in with the user account, the original user role settings take effect.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 188. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Configure local authentication for the Telnet user.

   For information about the configuration procedure, see "Configuring local AAA authentication mode for login users."
3. Create user role **role1** and configure rules for the user role:

   # Create user role **role1** and enter user role view.

   ```
   <Switch> system-view
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to execute all commands available for the features in feature group **L3**.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L3
   ```

   # Configure rule 2 to permit the user role to execute all commands that start with **display**.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```

   # Configure rule 3 to permit the user role to execute all commands that start with **super**.

   ```
   [Switch-role-role1] rule 3 permit command super *
   [Switch-role-role1] quit
   ```
4. Create user role **role2** and configure rules for the user role:

Create user role **role2** and enter user role view.

```
[Switch] role name role2
```

Configure rule 1 to permit the user role to execute all commands available for the features in feature group **L2**.

```
[Switch-role-role2] rule 1 permit execute read write feature-group L2
[Switch-role-role2] quit
```

5. Assign user role **role1** to device management user **telnetuser**:

Enter the view of the device management user.

```
[Switch] local-user telnetuser class manage
```

Assign user role **role1** to the user.

```
[Switch-luser-manage-telnetuser] authorization-attribute user-role role1
```

Remove the default user role **network-operator** from the user.

```
[Switch-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnetuser] quit
```

6. Configure temporary user role authorization:

Configure the authentication method as **local**. By default, the authentication method is **local**.

```
[Switch] super authentication-mode local
```

Set the password to **123456TESTplat&!** in plain text for obtaining user role **role2** temporarily.

```
[Switch] super password role role2 simple 123456TESTplat&!
```

Set the password to **987654TESTplat&!** in plain text for obtaining user role **network-operator** temporarily in the interactive mode.

```
[Switch] super password role network-operator
Password:
Confirm :
```

Verifying the configuration

1. Verify that the user role configuration is correct:

Display information about user role **role1**.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L3
  2       permit       command       display *
  3       permit       command       super *
  R:Read W:Write X:Execute
```

Display information about user role **role2**.

```
[Switch] display role name role2
Role: role2
```

```
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------
  1       permit RWX   feature-group L2
  R:Read W:Write X:Execute
```

Display information about user role **network-operator**.

```
[Switch] display role name network-operator
Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   deny         command       display history-command all
  sys-3   deny         command       display security-logfile summary
  sys-4   deny         command       system-view ; info-center securi
                                     ty-logfile switch-directory *
  sys-5   deny         command       security-logfile save
  R:Read W:Write X:Execute
```

2. Use the **display role feature-group** command to identify the features in feature groups **L2** and **L3**. (Details not shown.)
3. Telnet to the switch, and enter the username **telnetuser@bbb** and the user's password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute all commands available for the features in feature group **L3**. For example, create VPN instance **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
```

Verify that you can execute all commands that start with **display**. For example, use the **display clock** command to display date and time.

```
[Switch] display clock
09:31:56 UTC Tues 01/01/2013
[Switch] quit
```

5. Verify the temporary user role authorization configuration:

Use the **super** command to obtain user role **role2** temporarily.

```
<Switch> super role2
Password:
User privilege role is role2, and only those commands that authorized to the rol
e can be used.
<Switch>
```

Verify that you can execute all commands available for the features in feature group **L2**. For example, create VLAN 10 and assign Ten-GigabitEthernet 1/0/8 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port ten-gigabitethernet 1/0/8
[Switch-vlan10] quit
[Switch] quit
```

Verify that you cannot execute other commands except the commands of feature group **L2**. For example, use the **super** command for temporary user role authorization.

```
<Switch> super network-operator
Permission denied.
```

6. Log off the user, and use the same user account to re-Telnet to the switch. Verify that you can obtain the user role **network-operator** temporarily.

```
C:\Documents and Settings\user> telnet 192.168.1.50


******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
<Switch> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized
 to the role can be used.
<Switch>
```

Configuration files

```
#
 telnet server enable
#
```

```
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
 super password role role2 hash $h$6$D0kjHFktkktzgR5g$e673xFnIcKytCj6EDAw+pvwgh3
/ung3WNWHnrUTnXT862B+s7PaLfKTdil8ef71RBOvuJvPAZHjiLjrMPyWHQw==
 super password role network-operator hash $h$6$3s5KMmscn9hJ6gPx$IcxbNjUc8u4yxwR
m87b/Jki8BoPAxw/s5bEcPQjQj/cbbXwTVcnQGL91WOd7ssO2rX/wKzfyzAO5VhBTn9Q4zQ==
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 rule 3 permit command super *
#
role name role2
 rule 1 permit read write execute feature-group L2
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Example: Configuring login users to have access to ACL and QoS features

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 189:

- Department A and Department B use VLANs 100 to 199 and VLANs 200 to 299, respectively.
- The core switch uses the AAA server for Telnet user authentication and authorization.
- The Telnet users are authenticated in ISP domain **bbb**.
- Each department has a network administrator (a Telnet user) to manage the department network. The two network administrators use the usernames **admin-departA@bbb** and **admin-departB@bbb**.

The core switch and AAA server use the shared key **aabbcc** for secure RADIUS communication. The switch sends usernames with the domain name to the server.

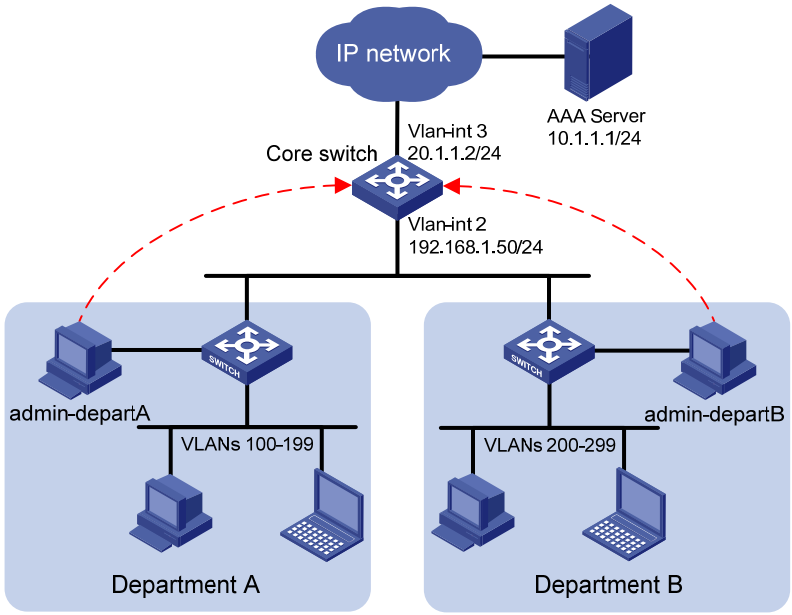
Configure network administrator **admin-departA@bbb** to have the following access permissions:

- Configure traffic control policies.
- Not access any VPN instances.
- Not access any VLANs except VLANs 100 to 199.
- Not access any interfaces except VLAN-interfaces 100 to 199.

Configure network administrator **admin-departB@bbb** to have the following access permissions:

- Configure traffic control policies.
- Not access any VPN instances.
- Not access any VLANs except VLANs 200 to 299.
- Not access any interfaces except VLAN-interfaces 200 to 299.

Figure 189 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the users can Telnet to the switch. By default, the Telnet server function is disabled.
- Create and configure user roles to control access permissions of network administrators:
  a. Create user roles **depart-admin**, **departA-resource**, and **departB-resource** on the switch.
  b. Configure access permissions for the user roles.
     – Configure **depart-admin** to have access to all commands of the **acl** and **qos** features.
     – Configure **departA-resource** to have access to VLANs 100 to 199 and VLAN-interfaces 100 to 199.
     – Configure **departB-resource** to have access to VLANs 200 to 299 and VLAN-interfaces 200 to 299.
  c. Configure the server to assign user roles **depart-admin** and **departA-resource** to **admin-departA@bbb** and assign user roles **depart-admin** and **departB-resource** to **admin-departB@bbb**.

Configuration restrictions and guidelines

When you configure the remote AAA authentication mode, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- RADIUS user authorization information is piggybacked in authentication responses. Use the same RADIUS scheme for authentication and authorization.

Configuration procedures

1. Assign an IP address to each interface. Make sure the devices in Figure 189 can reach each other. (Details not shown.)
2. Enable the Telnet server function.

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

3. Enable scheme authentication on VTY user interfaces 0 to 15.

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

4. Configure the RADIUS scheme:

   # Create RADIUS scheme **rad**.

```
[Switch] radius scheme rad
```

   # Configure the AAA server at 10.1.1.1 as the primary authentication server. Set the authentication port to **1812**.

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

   # Set the shared key to **aabbcc** in plain text for secure RADIUS communication.

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

5. Configure the ISP domain:

   # Create ISP domain **bbb**.

```
[Switch] domain bbb
```

   # Configure the ISP domain to use RADIUS authentication and authorization for login users.

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

6. Configure user roles:

   # Create user role **depart-admin**, and allow the user role to access commands of the **qos** and **acl** features.

```
[Switch] role name depart-admin
[Switch-role-depart-admin] rule 1 permit read write execute feature qos
[Switch-role-depart-admin] rule 2 permit read write execute feature acl
```

   # Deny the access of user role **depart-admin** to any interfaces, VLANs, and VPN instances.

```
[Switch-role-depart-admin] vlan policy deny
[Switch-role-departA-resource-vlan-policy] quit
[Switch-role-depart-admin] interface policy deny
[Switch-role-departA-resource-interface-policy] quit
[Switch-role-depart-admin] vpn policy deny
[Switch-role-departA-resource-vpn-policy] quit
[Switch-role-depart-admin] quit
```

   # Create user role **departA-resource**, and deny the user role to access any VLANs and interfaces except VLANs 100 to 199 and VLAN-interfaces 100 to 199.

```
[Switch] role name departA-resource
[Switch-role-departA-resource] vlan policy deny
```

```
[Switch-role-departA-resource-vlan-policy] permit vlan 100 to 199
[Switch-role-departA-resource-vlan-policy] quit
[Switch-role-departA-resource] interface policy deny
[Switch-role-departA-resource-interface-policy] permit interface Vlan-interface 100
to Vlan-interface 199
[Switch-role-departA-resource-interface-policy] quit
[Switch-role-departA-resource] quit
```

Create user role **departB-resource**, and deny the user role to access any VLANs and interfaces except VLANs 200 to 299 and VLAN-interfaces 200 to 299.

```
[Switch] role name departB-resource
[Switch-role-departB-resource] vlan policy deny
[Switch-role-departB-resource-vlan-policy] permit vlan 200 to 299
[Switch-role-departB-resource-vlan-policy] quit
[Switch-role-departB-resource] interface policy deny
[Switch-role-departB-resource-interface-policy] permit interface Vlan-interface 200
to Vlan-interface 299
[Switch-role-departB-resource-interface-policy] quit
[Switch-role-departB-resource] quit
```

7. Configure the RADIUS server:

Add the NAS IP address and shared key configuration to the **clients.conf** configuration file.

```
client 20.1.1.2/24 {
  secret   = aabbcc
```

Add the account configuration of **admin-departA** and **admin-departB** to the **users** file.

```
admin-departA
  Cleartext-Password := "admin-departA"
  Service-Type = Login-User,
  Login-Service = Telnet,
  Cisco-AVPair = "shell:roles=\"depart-admin\" \"departA-resource\""

admin-departB
  Cleartext-Password := "admin-departB"
  Service-Type = Login-User,
  Login-Service = Telnet,
  Cisco-AVPair = "shell:roles=\"depart-admin\" \"departB-resource\""
```

For more information about the server configuration, see the configuration guide for the server.

Verifying the configuration

1. Verify that the user role configuration is correct:

Display information about user role **depart-admin**.

```
[Switch] display role name depart-admin
Role: depart-admin
  Description:
  VLAN policy: deny
  Interface policy: deny
  VPN instance policy: deny
  ----------------------------------------------------------------------
```

```
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------
  1       permit RWX   feature       qos
  2       permit RWX   feature       acl
  R:Read W:Write X:Execute
```

Display information about user role **departA-resource**.

```
[Switch] display role name departA-resource
Role: departA-resource
  Description:
  VLAN policy: deny
  Permitted VLANs: 100 to 199
  Interface policy: deny
  Permitted interfaces: Vlan-interface100 to Vlan-interface199
  VPN instance policy: permit (default)
```

Display information about user role **departB-resource**.

```
[Switch] display role name departB-resource
Role: departB-resource
  Description:
  VLAN policy: deny
  Permitted VLANs: 200 to 299
  Interface policy: deny
  Permitted interfaces: Vlan-interface200 to Vlan-interface299
  VPN instance policy: permit (default)
```

2. Telnet to the switch, and enter the username **admin-departA@bbb** and the password. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: admin-departA@bbb
Password:
<Switch>
```

3. Verify that you have the access permissions of user roles **depart-admin** and **departA-resource**. For example:

Create ACL 3000.

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

Configure a rule for ACL 3000 to permit FTP packets.

```
[Switch-acl-adv-3000] rule permit tcp destination-port eq ftp-data
[Switch-acl-adv-3000] quit
```

Create traffic class 1.

```
[Switch] traffic classifier 1
```

Define a match criterion for traffic class 1 to match ACL 3000.

```
[Switch-classifier-1] if-match acl 3000
[Switch-classifier-1] quit
```

Create traffic behavior 1.

```
[Switch] traffic behavior 1
```

Configure a CAR action for the traffic behavior, and set the CIR to 2000 kbps.

```
[Switch-behavior-1] car cir 2000
[Switch-behavior-1] quit
```

Create QoS policy 1, and associate traffic class 1 with traffic behavior 1 in the QoS policy.

```
[Switch] qos policy 1
[Switch-qospolicy-1] classifier 1 behavior 1
[Switch-qospolicy-1] quit
```

Verify that you can apply the QoS policy to VLANs 100 to 199. In this example, apply QoS policy 1 to the inbound direction of VLANs 100 to 107.

```
[Switch] qos vlan-policy 1 vlan 100 to 107 inbound
```

Verify that you cannot apply the QoS policy to other VLANs except VLANs 100 to 199. In this example, apply the QoS policy to the inbound direction of VLANs 200 to 207.

```
[Switch] qos vlan-policy 1 vlan 200 to 207 inbound
Permission denied.
```

4. Use username **admin-departB@bbb** to Telnet to the switch. Verify that you have the access permissions of user roles **depart-admin** and **departB-resource**. For example:

Create ACL 3001.

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

Configure a rule for ACL 3000 to permit FTP packets.

```
[Switch-acl-adv-3001] rule permit tcp destination-port eq ftp-data
[Switch-acl-adv-3001] quit
```

Create traffic class 2.

```
[Switch] traffic classifier 2
```

Define a match criterion for traffic class 2 to match ACL 3001.

```
[Switch-classifier-2] if-match acl 3001
[Switch-classifier-2] quit
```

Create traffic behavior 2.

```
[Switch] traffic behavior 2
```

Configure a CAR action for the traffic behavior, and set the CIR to 2000 kbps.

```
[Switch-behavior-2] car cir 2000
[Switch-behavior-2] quit
```

Create QoS policy 2, and associate traffic class 2 with traffic behavior 2 in the QoS policy.

```
[Switch] qos policy 2
[Switch-qospolicy-2] classifier 1 behavior 2
[Switch-qospolicy-2] quit
```

Verify that you can apply the QoS policy to VLANs 200 to 299. In this example, apply QoS policy 2 to the inbound direction of VLANs 200 to 207.

```
[Switch] qos vlan-policy 2 vlan 200 to 207 inbound
```

Verify that you cannot apply the QoS policy to other VLANs except VLANs 200 to 299. In this example, apply the QoS policy to the inbound direction of VLANs 100 to 107.

```
[Switch] qos vlan-policy 2 vlan 100 to 107 inbound
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Vlan-interface3
 ip address 20.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZIcJhzscTHLA4WasBVh0UOw==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
#
role name depart-admin
 rule 1 permit read write execute feature qos
 rule 2 permit read write execute feature acl
 vlan policy deny
 interface policy deny
 vpn-instance policy deny
#
role name departA-resource
 vlan policy deny
  permit vlan 100 to 199
 interface policy deny
  permit interface Vlan-interface100 to Vlan-interface199
#
role name departB-resource
```

```
 vlan policy deny
  permit vlan 200 to 299
 interface policy deny
  permit interface Vlan-interface200 to Vlan-interface299
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Appendix Configuring authentication modes for login users

In this chapter, users use the Telnet method to log in to the switch. Configure authentication modes for other login users in the same way the authentication mode is configured for Telnet users.

Configuring none authentication mode for login users

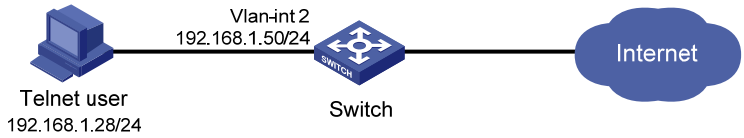
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 190, the network is secure, and the Telnet user can log in to the switch without authentication.

Figure 190 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Configure the **none** authentication mode on VTY user interfaces, so the Telnet user (a VTY user) can log in to the switch without authentication. By default, the authentication mode is **password**.

Configuration procedures

Assign an IP address to VLAN-interface 2, as shown in Figure 190. Make sure the Telnet user and switch can reach each other. (Details not shown.)

Enable the Telnet server function.

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

Enable the **none** authentication mode on VTY user interfaces 0 to 15.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode none
[Switch-ui-vty0-15] quit
```

Verifying the configuration

Telnet to the switch. Verify that you can log in to the switch without authentication.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode none
 user-role network-operator
#
```

Configuring password authentication mode for login users

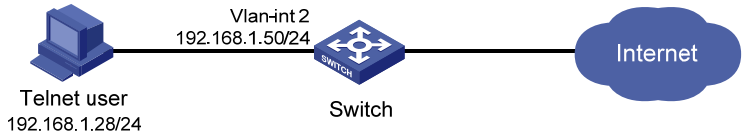
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 191, the Telnet user can access the switch only after it passes password authentication.

Figure 191 Network diagram



Requirements analysis

To meet the network requirements, you must perform the following tasks:

- Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.
- Configure the **password** authentication mode on VTY user interfaces and specify a password, so the Telnet user (a VTY user) can log in to the switch after it enters the correct password.

Configuration procedures

Assign an IP address to VLAN-interface 2, as shown in Figure 191. Make sure the Telnet user and switch can reach each other. (Details not shown.)

Enable the Telnet server function.

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

Enable password authentication on VTY user interfaces. By default, the authentication mode is **password**.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode password
```

Set the password to **123456** in plain text on VTY user interfaces.

```
[Switch-ui-vty0-15] set authentication password simple 123456
[Switch-ui-vty0-15] quit
```

Verifying the configuration

Telnet to the switch. Verify that you can log in to the switch after you enter the password **123456**.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Password:
<Switch>
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
user-interface vty 0 15
 user-role network-operator
 set authentication password hash $h$6$vaSj2xKc8yFiNdfQ$Jzb3PXo2ltTPcgyTQJZShe4j
kKSZqJUVhjP634Wol/Qx8TLU748IHoeui0w5n/XRzpNqbNnpxikym39gGJCwYw==
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Configuring local AAA authentication mode for login users

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

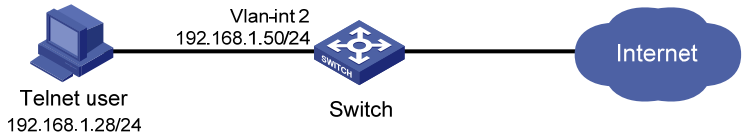
Network requirements

As shown in Figure 192, configure the switch to perform local authentication and authorization for login users, including the Telnet user.

Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses local authentication and authorization for login users.

Add a device management user named **telnetuser** and specify the password as **aabbcc**. The Telnet user must use username **telnetuser@bbb** and password **aabbcc** to log in to the switch.

Figure 192 Network diagram



Requirements analysis

Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.

Configuration restrictions and guidelines

To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.

Configuration procedures

1. Assign an IP address to VLAN-interface 2, as shown in Figure 192. Make sure the Telnet user and switch can reach each other. (Details not shown.)
2. Enable the Telnet server function.

   ```
   <switch> system-view
   [Switch] telnet server enable
   ```
3. Configure the local AAA authentication mode:

Enable scheme authentication on VTY user interfaces.

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

Create ISP domain **bbb**.

```
[Switch] domain bbb
```

Configure local authentication and authorization for login users of the ISP domain.

```
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit
```

4. Configure the Telnet user:

Create device management user **telnetuser**.

```
[Switch] local-user telnetuser class manage
```

Set the user password to **aabbcc** in plain text.

```
[Switch-luser-manage-telnetuser] password simple aabbcc
```

Specify Telnet service for the user.

```
[Switch-luser-manage-telnetuser] service-type telnet
[Switch-luser-manage-telnetuser] quit
```

Verifying the configuration

Telnet to the switch, and enter the username **telnetuser@bbb** and password **aabbcc**. Verify that you can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: telnetuser@bbb
Password:
<Switch>
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
```

```
 port access vlan 2
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
local-user telnetuser class manage
 password hash $h$6$VLhDcJkrZfRjyTMa$oURQbSVkWRHt5xzWUXc6BBTNcJupHSysfK8aX8x8Eee
HWU3g1AljSqQxlPmXOYBhpkhD1jCL/0PPRqElCy3rXA==
 service-type telnet
 authorization-attribute user-role network-operator
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

Configure remote AAA authentication mode for login users

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

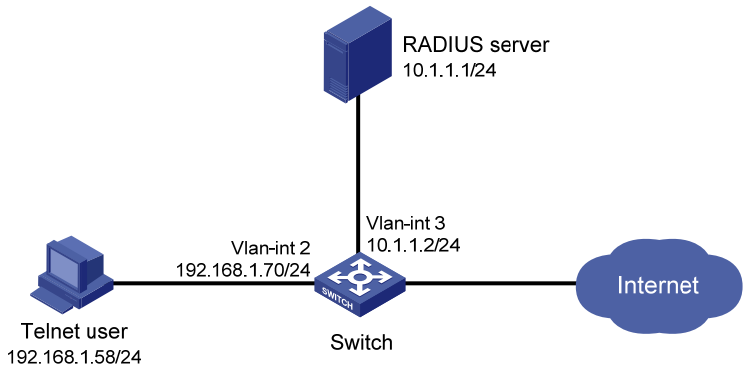
As shown in Figure 193, configure the switch to perform the following operations:

- Use the FreeRADIUS server at 10.1.1.1/24 for user authentication and authorization, including the Telnet user.
- Use the shared key **aabbcc** for secure RADIUS communication between the switch and the server.
- Send usernames with domain names to the server.

Create ISP domain **bbb**, in which the Telnet user is authenticated. The ISP domain uses RADIUS authentication and authorization for login users.

The Telnet user uses the username **hello@bbb**.

Figure 193 Network diagram



Requirements analysis

Enable the Telnet server function on the switch, so the user can Telnet to the switch. By default, the Telnet server function is disabled.

Configuration restrictions and guidelines

When you configure RADIUS authentication, follow these restrictions and guidelines:

- To delete the ISP domain that functions as the default ISP domain, you must first change it to a non-default ISP domain by using the **undo domain default enable** command.
- RADIUS user authorization information is piggybacked in authentication responses. Use the same RADIUS scheme for authentication and authorization.

Configuration procedures

Configuring the switch

1. Assign an IP address to each interface, as shown in Figure 193. Make sure the Telnet user, switch, and RADIUS server can reach each other. (Details not shown.)
2. Enable the Telnet server function.

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

3. Enable scheme authentication on VTY user interfaces.

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

4. Configure the RADIUS scheme:

   # Create RADIUS scheme **rad**.

```
[Switch] radius scheme rad
```

   # Specify the RADIUS server at 10.1.1.1 as the primary authentication server. Set the authentication port to **1812**.

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

   # Set the shared key to **aabbcc** in plain text for secure RADIUS communication.

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

5. Configure the authentication ISP domain:

   # Create ISP domain **bbb**.

   ```
   [Switch] domain bbb
   ```

   # Configure RADIUS authentication and authorization for login users of the ISP domain.

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

Configuring the RADIUS server

Configure the RADIUS server in the same way the server is configured in "Example: Configuring login users to have access to specific features in specific VPN instances."

Verifying the configuration

Telnet to the switch, enter the username **hello@bbb** and the user password. Verify that the user can log in to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.70

******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: hello@bbb
Password:
<Switch>
```

Configuration files

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.70 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
```

```
 port access vlan 3
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZIcJhzscTHLA4WasBVh0UOw==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
#
```

NOTE:

Whether the login password is displayed in plain text or encrypted text depends on the software version.

sFlow configuration examples

This chapter provides sFlow configuration examples.

Example: Configuring sFlow

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

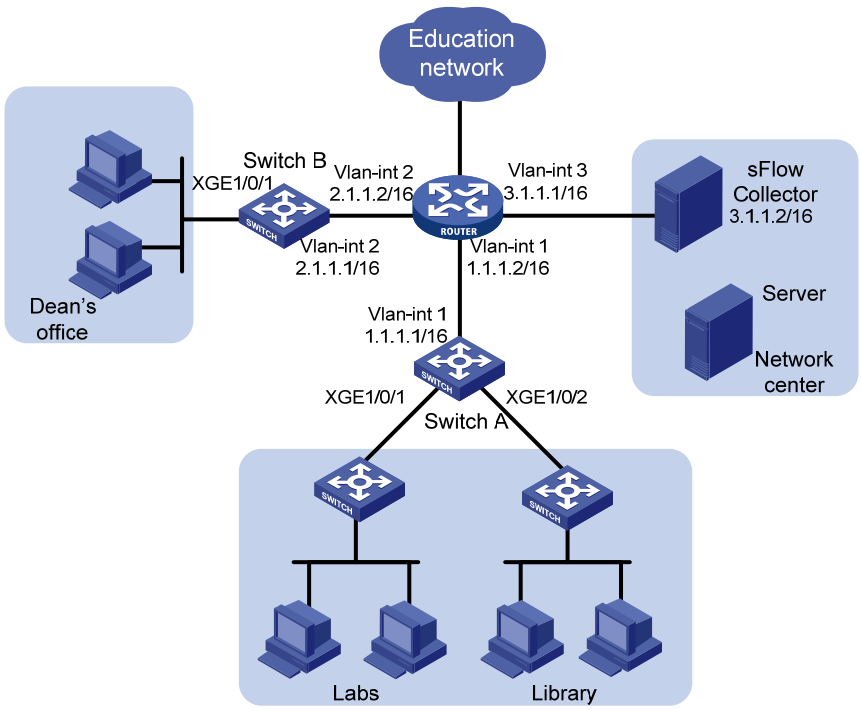
Network requirements

As shown in Figure 194, configure flow sampling and counter sampling on Switch A and Switch B to monitor traffic on the ports:

- Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 of Switch A.
- Ten-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 194 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 ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] sflow counter interval 120
[SwitchA-Ten-GigabitEthernet1/0/1] sflow counter collector 1
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] sflow counter interval 120
[SwitchA-Ten-GigabitEthernet1/0/2] sflow counter collector 1
[SwitchA-Ten-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-Ten-GigabitEthernet1/0/1] sflow sampling-rate 100000
[SwitchA-Ten-GigabitEthernet1/0/1] sflow flow collector 1
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] sflow sampling-rate 100000
[SwitchA-Ten-GigabitEthernet1/0/2] sflow flow collector 1
[SwitchA-Ten-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 ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] sflow counter interval 30
[SwitchB-Ten-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-Ten-GigabitEthernet1/0/1] sflow sampling-rate 20000
[SwitchB-Ten-GigabitEthernet1/0/1] sflow flow collector 1
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the sFlow configuration and operation information. This example uses Switch A:

```
[SwitchA] display sflow
sFlow datagram version: 5
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
Port information:
Interface      CID   Interval(s) FID   MaxHLen Rate       Mode      Status
XGE1/0/1       1     120         1     128     100000     Random    Suspended
XGE1/0/2       1     120         1     128     100000     Random    Suspended
```

Configuration files

- Switch A:

```
#
 sflow agent ip 1.1.1.1
 sflow collector 1 ip 3.1.1.2 port 5000
#
interface Ten-GigabitEthernet1/0/1
 sflow sampling-rate 100000
 sflow flow collector 1
 sflow counter interval 120
 sflow counter collector 1
#
interface Ten-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 Ten-GigabitEthernet1/0/1
 sflow sampling-rate 20000
 sflow flow collector 1
 sflow counter interval 30
 sflow counter collector 1
#
```

SNMP configuration examples

This chapter provides SNMP configuration examples.

Example: Configuring SNMPv1/v2c

Applicable product matrix

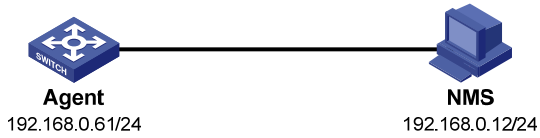
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 195, configure SNMPv1 to meet the following requirements:

- The NMS can manage the SNMP agent.
- The agent can automatically send notifications to report events to the NMS.

Figure 195 Network diagram



Configuration restrictions and guidelines

When you configure SNMP, follow these restrictions and guidelines:

- SNMPv1 and SNMPv2c configuration procedures are the same. This example uses SNMPv1.
- The SNMP settings on the agent and the NMS must match.
- The NMS configuration varies by the NMS software. This example uses IMC PLAT 7.0. For more information about configuring the NMS, see the NMS manual.

Configuration procedures

Configuring the agent

Enable SNMPv1.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v1
```

Create the read-only community **public** and the read and write community **private**.

```
[Agent] snmp-agent community read public
```

```
[Agent] snmp-agent community write private
```

Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

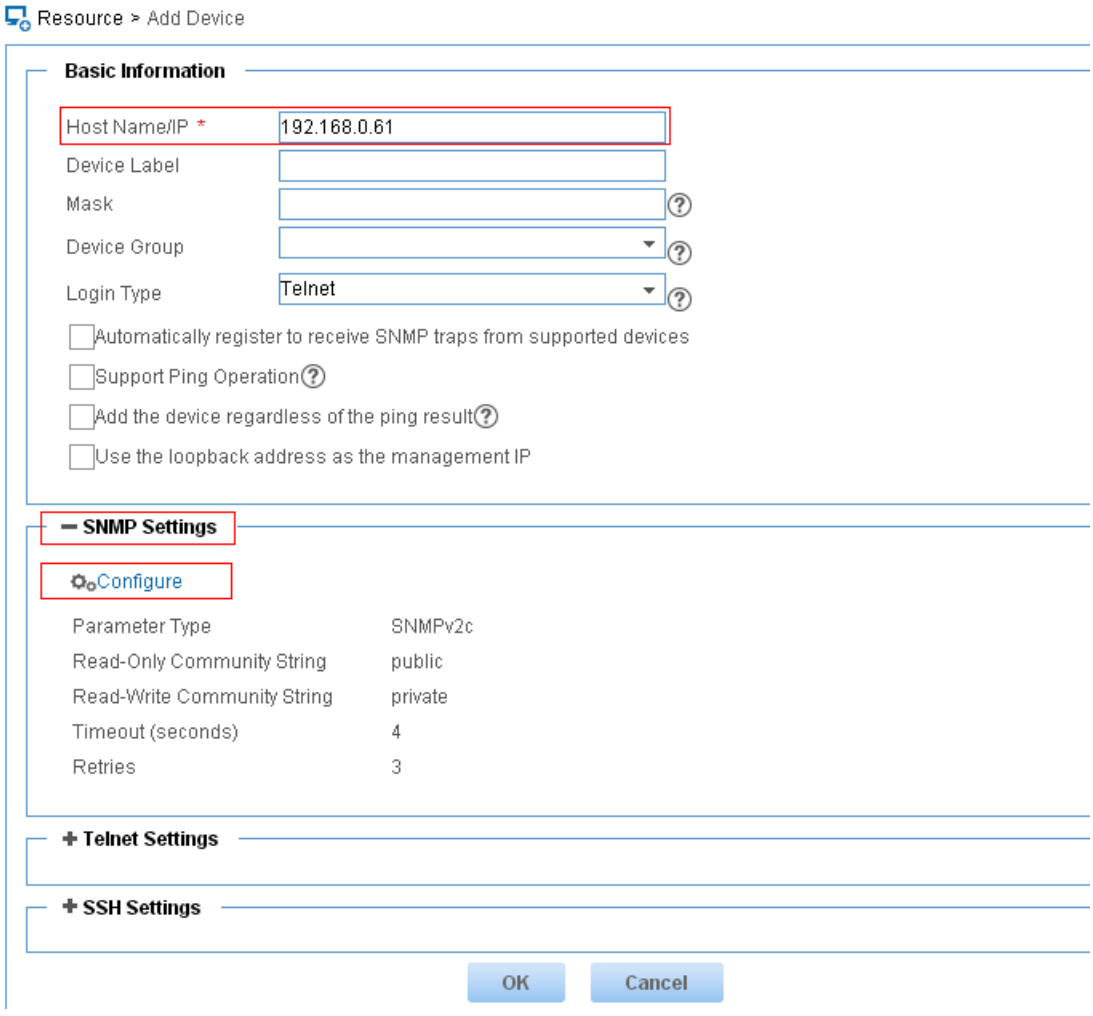
Configure the NMS at 192.168.0.12 as an SNMP notification destination, and use **public** as the community name.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.0.12 params securityname
public v1
```

Configuring the NMS

1. Log in to IMC, and do the following:
   a. Click the **Resource** tab, and select **Resource Management** > **Add Device** from the navigation tree.
   b. On the **Add Device** page, enter **192.168.0.61** for **Host Name/IP**.
   c. Click **SNMP Settings**, and then click **Configure**.

Figure 196 Adding a device

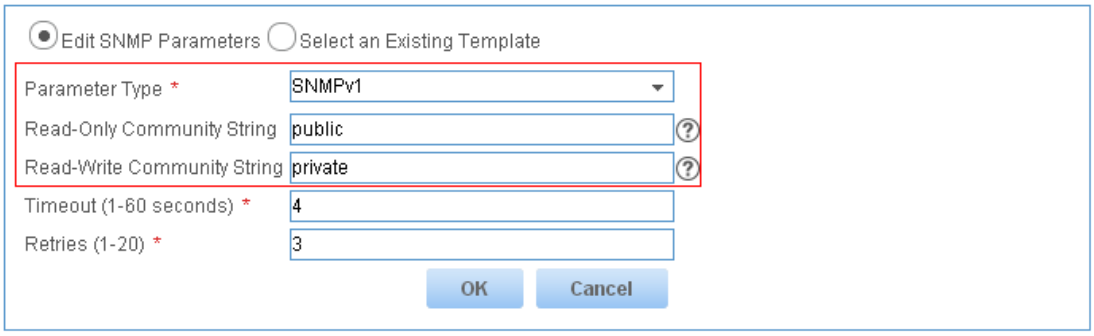


2. On the page that appears, do the following:
   a. Select **SNMPv1** from the **Parameter Type** list.
   b. Enter **public** for **Read-Only Community String** to configure the read-only community name.

c. Enter **private** for **Read-Write Community String** to configure the read and write community name.

d. Click **OK** to return to the **Add Device** page.

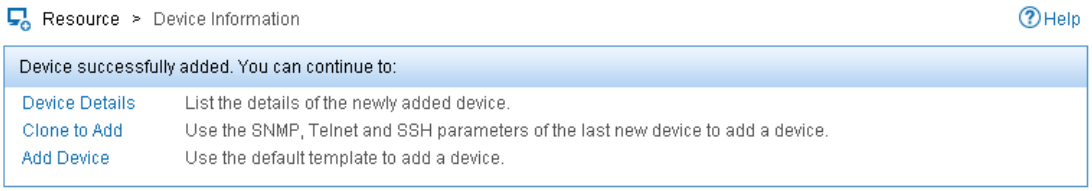
Figure 197 Editing SNMP parameters



3. On the **Add Device** page, click **OK**.

   The **Device Information** page shows that the device has been added.

Figure 198 Device Information page



Verifying the configuration

Click the **Resource** tab, and select **View Management** > **Device View** from the navigation tree. On the page that appears, you can see the device you have added.

Execute the **shutdown** command on VLAN-interface 1 on the device. You can see the link state change notifications sent to the NMS.

Configuration files

```
#
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version v1 v3
 snmp-agent target-host trap address udp-domain 192.168.0.12 params securityname public
#
```

Example: Configuring SNMPv3

Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

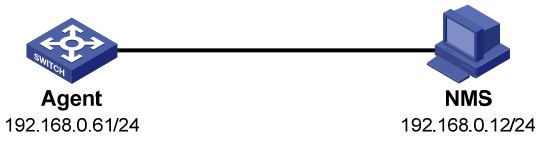
Network requirements

As shown in Figure 199, configure SNMPv3 to meet the following requirements:

- The NMS can monitor and manage the interface status of the agent.
- The agent can automatically send notifications to report events to the NMS.

The NMS and the agent perform authentication when they set up an SNMP session. They also encrypt the SNMP packets between them.

Figure 199 Network diagram



Configuration restrictions and guidelines

When you configure SNMP, follow these restrictions and guidelines:

- The SNMP settings on the agent and the NMS must match.
- The NMS configuration varies by the NMS software. This example uses IMC PLAT 7.0. For more information about configuring the NMS, see the NMS manual.

Configuration procedures

Configuring the agent

Enable SNMPv3.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

Do the following:

- Create the SNMPv3 group **managev3group**.
- Assign the authentication with privacy security model to the group.
- Specify the read-only, read and write, and notify MIB views all as **ViewDefault**.

```
[Agent] snmp-agent group v3 managev3group privacy read-view ViewDefault write-view
ViewDefault notify-view ViewDefault
```

Do the following:

- Add the user **managev3user** to the SNMPv3 group **managev3group**.
- Set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and privacy key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Enable notifications.

```
[Agent] snmp-agent trap enable
```

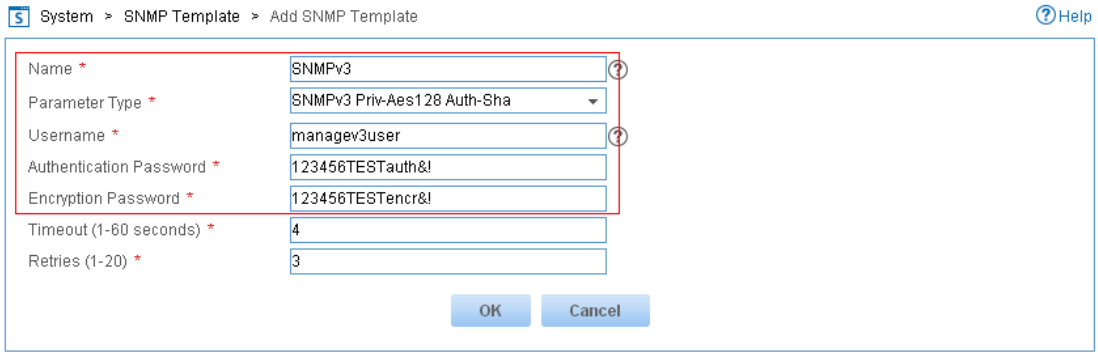
Specify the NMS at 192.168.0.12 as a notification destination, and set the username to **managev3user** for the notifications.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.0.12 params securityname
managev3user v3 privacy
```

Configuring the NMS

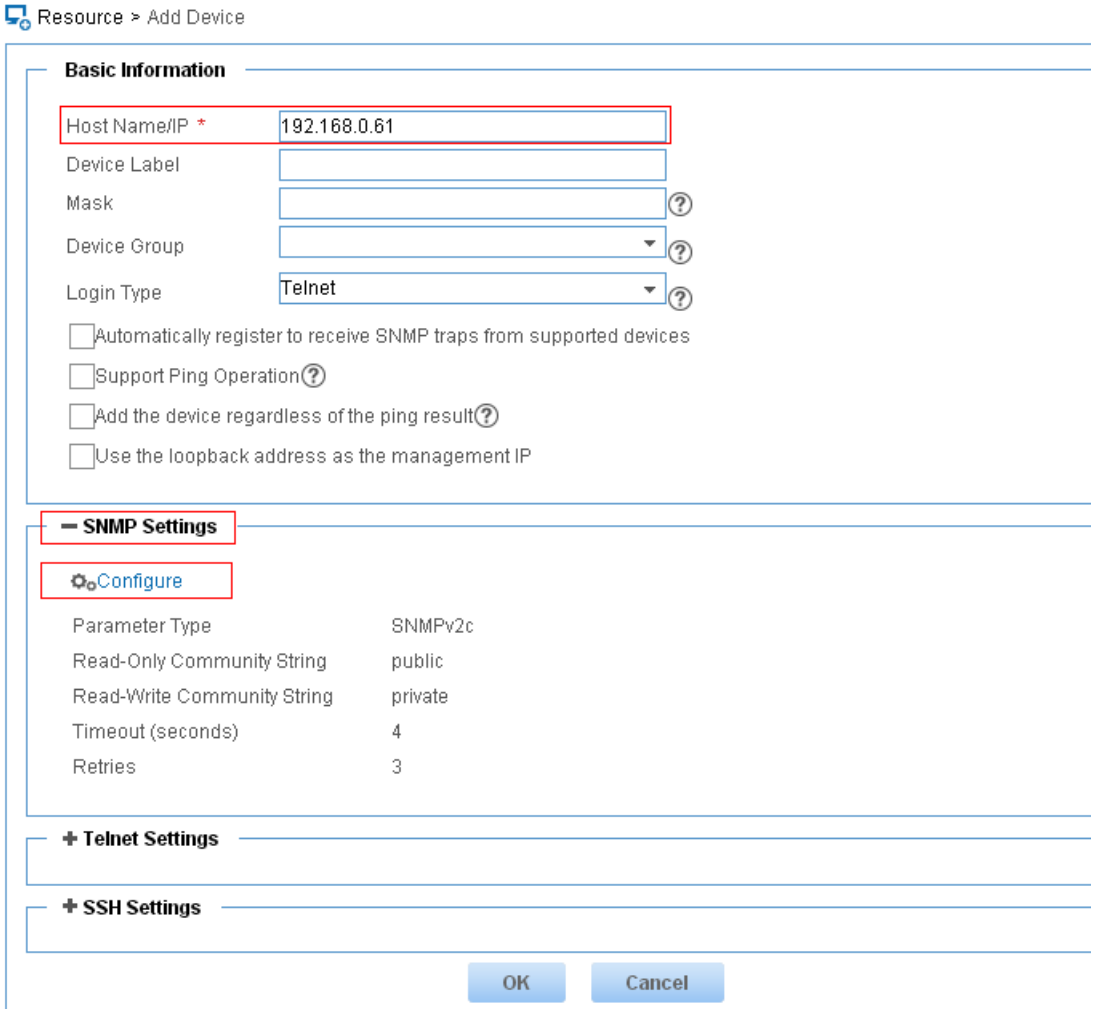
1. Log in to IMC, and do the following:
   a. Click the **System** tab, and select **Resource Management** > **SNMP Template** from the navigation tree.
   b. On the **SNMP Template** page, click **Add**.
2. On the **Add SNMP Template** page, do the following:
   a. Enter **SNMPv3** for **Name**.
   b. Select **SNMPv3 Priv-Aes128 Auth-Sha** from the **Parameter Type** list.
   c. Enter **managev3user** for **Username**.
   d. Enter **123456TESTauth&!** for **Authentication Password**.
   e. Enter **123456TESTencr&!** for **Encryption Password**.
   f. Click **OK**.

Figure 200 Adding an SNMP template



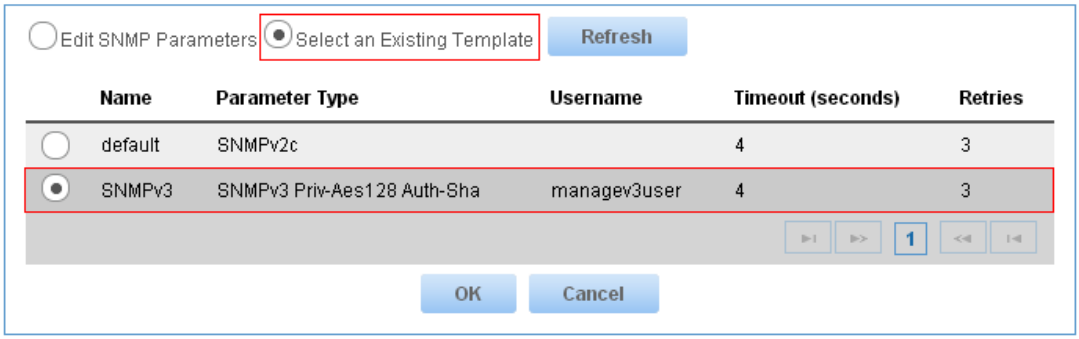
3. On the page that appears, do the following:
   a. Click the **Resource** tab, and select **Resource Management** > **Add Device** from the navigation tree.
   b. On the **Add Device** page, enter **192.168.0.61** for **Host Name/IP**.
   c. Click **SNMP Settings**, and then click **Configure**.

Figure 201 Adding a device



4. On the page that appears, do the following:
   a. Select the option **Select an Existing Template**.
   b. Select the template named **SNMPv3**.
   c. Click **OK** to return to the **Add Device** page.

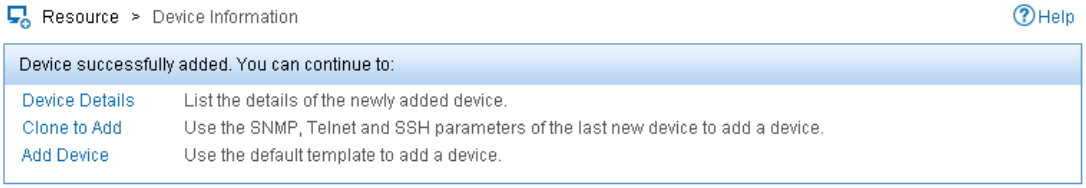
Figure 202 Selecting an existing template



5. On the **Add Device** page, click **OK**.

   The **Device Information** page shows that the device has been added.

Figure 203 Device Information page



Verifying the configuration

Click the **Resource** tab, and select **View Management** > **Device View** from the navigation tree. On the page that appears, you can see the device you have added.

Execute the **shutdown** command on VLAN-interface 1 on the device. You can see the link state change notifications sent to the NMS.

Configuration files

```
#
 snmp-agent sys-info version v3
 snmp-agent group v3 managev3group privacy write-view ViewDefault notify-view ViewDefault
 snmp-agent target-host trap address udp-domain 192.168.0.12 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
```

Software upgrade configuration examples

This chapter provides examples for each task in the software upgrade procedure for an IRF fabric without using ISSU.

Software upgrade procedure includes software upgrade preparation, file transfer (FTP or TFTP), and software loading.

Example: Preparing for software upgrade

Applicable product matrix

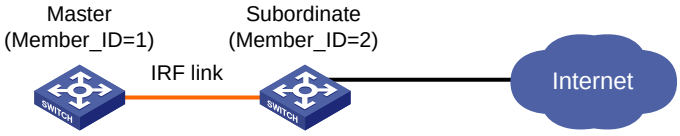
Product series	Software version
HP 5900	Release 2210
HP 5920	Release 2208P01

Network requirements

As shown in Figure 204:

- Verify that the member switches in the IRF fabric have sufficient storage space for software images.
- Back up the configuration files.

Figure 204 Network diagram



Configuration procedures

Display files and subdirectories in the root directory of the flash memory on the master switch.

```
<Sysname> dir
Directory of flash:
   0 -rw-    52922368 Jan 01 2011 01:31:49   5900_r2208p01.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
```

```
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (191248 KB free)
```

Display files and subdirectories in the root directory of the flash memory on the subordinate switch.

```
<Sysname> dir slot2#flash:/
Directory of slot2#flash:
   0 -rw-    52922368 Jan 01 2011 01:31:49   5900_r2208p01.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (191248 KB free)
```

Delete unused files to ensure sufficient storage space. In this example, delete **5900_r2208p01.ipe** from the master switch.

```
<Sysname>delete /unreserved flash:/5900_r2208p01.ipe
The file cannot be restored. Delete flash:/5900_r2208p01.ipe?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/5900_r2208p01.ipe...Done.
```

Delete unused files to ensure sufficient storage space. In this example, delete **5900_r2208p01.ipe** from the subordinate switch.

```
<Sysname> delete /unreserved slot2#flash:/5900_r2208p01.ipe
The file cannot be restored. Delete flash:/5900_r2208p01.ipe?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/5900_r2208p01.ipe...Done.
```

Copy the configuration file **startup.cfg** to **startup_bak.cfg** on the master switch.

```
<Sysname> copy startup.cfg startup_bak.cfg
Copy flash:/startup.cfg to flash:/startup_bak.cfg?[Y/N]:y
Copying file flash:/startup.cfg to flash:/startup_bak.cfg...Done.
```

Verifying the configuration

Display files and subdirectories in the root directory of the flash memories on the IRF member devices.

```
<Sysname> dir /all-filesystems
Directory of flash:
   0 drw-           - Jan 01 2011 00:47:50   core
   1 drw-           - Jan 01 2011 00:00:30   diagfile
   2 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
```

```
   3 drw-           - Jan 02 2000 00:00:07   logfile
   4 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   5 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   6 drw-           - Jan 01 2000 00:00:07   seclog
   7 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   8 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
   9 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  10 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (244160 KB free)

Directory of slot2#flash:
   0 drw-           - Jan 01 2011 00:47:50   core
   1 drw-           - Jan 01 2011 00:00:30   diagfile
   2 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   3 drw-           - Jan 02 2000 00:00:07   logfile
   4 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   5 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   6 drw-           - Jan 01 2000 00:00:07   seclog
   7 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   8 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
   9 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  10 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (244160 KB free)
```

Configuration files

The system does not save file operations to a configuration file.

Example: Downloading software from an FTP server

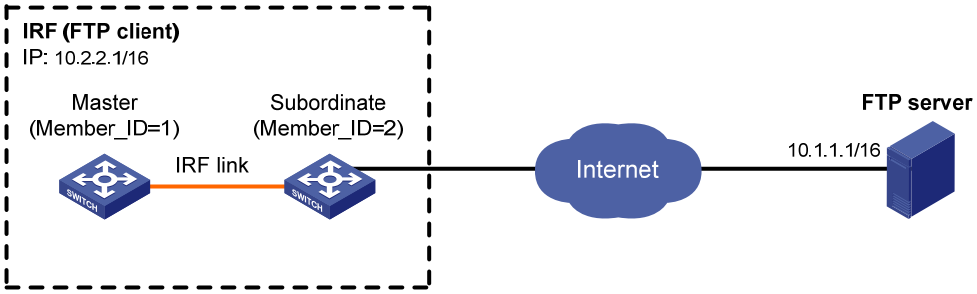
Applicable product matrix

Product series	Software version
HP 5900	Release 2210
HP 5920	Release 2208P01

Network requirements

As shown in Figure 205, use the IRF fabric as an FTP client to download software images from an FTP server.

Figure 205 Network diagram



Configuration restrictions and guidelines

When you use FTP to transfer software, you must set the file transfer mode to binary.

Configuration procedures

This example assumes that the FTP server and the IRF fabric can ping each other. A user account and a working directory have been configured on the FTP server.

Use the user name and password of the user account to log in to the FTP server.

```
<Sysname>ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
```

Set the file transfer mode to binary.

```
ftp> binary
200 Type is Image (Binary)
```

Download the startup image file from the FTP server to the root directory of the flash memory on the master switch.

```
ftp> get 5900_r2210.ipe
227 Entering Passive Mode (10,1,1,1,8,17)
150 "C:\5900_r2210.ipe" file ready to send (52922368 bytes) in IMAGE / Binary mode
226 Transfer finished successfully.
52922368 bytes received in 107 seconds (484.4 kbyte/s)
```

Download the startup image file from the FTP server to the root directory of the flash memory on the subordinate switch.

```
ftp> get 5900_r2210.ipe slot2#flash:/5900_r2210.ipe
```

```
227 Entering Passive Mode (10,1,1,1,8,17)
150 "C:\5900_r2210.ipe" file ready to send (52922368 bytes) in IMAGE / Binary mode
226 Transfer finished successfully.
52922368 bytes received in 107 seconds (484.4 kbyte/s)
```

Close the FTP connection.

```
ftp> bye
```

Verifying the configuration

Display files and subdirectories in the root directory of the flash memories on the IRF member devices.

```
<Sysname> dir /all-filesystems
Directory of flash:
   0 -rw-    52922368 Jan 01 2011 08:07:22   5900_r2210.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  11 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (199240 KB free)

Directory of slot2#flash:
   0 -rw-    52922368 Jan 01 2011 08:07:22   5900_r2210.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  11 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (199240 KB free)
```

Configuration files

The system does not save the commands used in this procedure to a configuration file.

Example: Uploading software to the IRF fabric from an FTP client

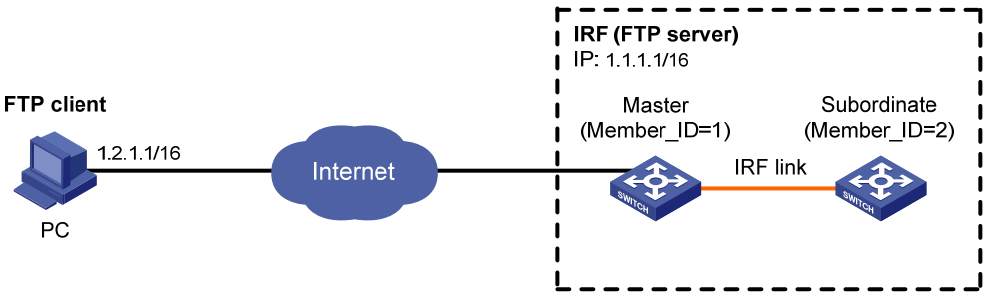
Applicable product matrix

Product series	Software version
HP 5900	Release 2210
HP 5920	Release 2208P01

Network requirements

As shown in Figure 206, the IRF fabric is an FTP server. Use an FTP client to upload software images to the IRF fabric.

Figure 206 Network diagram



Configuration restrictions and guidelines

When you use FTP to transfer software, you must set the file transfer mode to binary.

Configuration procedures

This example assumes that the FTP client and the IRF fabric can ping each other.

1. Configure the IRF fabric:

   # Add a local user account.

   ```
   <Sysname> system-view
   [Sysname] local-user abc class manage
   ```

   # Set the username to **abc** and the password to **123456** for the user account.

   ```
   [Sysname-luser-abc] password simple 123456
   ```

Assign the network-admin user role to the user account, and specify the root directory of the flash memory as the working directory for FTP access.

```
[Sysname-luser-abc] authorization-attribute user-role network-admin work-directory flash:/
```

Assign FTP service to the user account.

```
[Sysname-luser-abc] service-type ftp
[Sysname-luser-abc] quit
```

Enable the FTP server function.

```
[Sysname] ftp server enable
[Sysname] quit
```

2. Configure the FTP client:

Use the username **abc** and the password **123456** to log in to the IRF fabric.

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

Set the file transfer mode to binary.

```
ftp> binary
200 TYPE is now 8-bit binary
```

Transfer the file **5900_r2210.ipe** to the root directory of the flash memory on the master switch.

```
ftp> put 5900_r2210.ipe
```

Close the FTP connection.

```
ftp> bye
```

3. Configure the IRF:

Copy the file **5900_r2210.ipe** from the root directory of the flash memory on the master switch to the root directory of the flash memory on the subordinate switch.

```
<Sysname> copy 5900_r2210.ipe slot2#flash:/
Copy flash:/5900_r2210.ipe to slot2#flash:/5900_r2210.ipe?[Y/N]:y
Copying file flash:/5900_r2210.ipe to slot2#flash:/5900_r2210.ipe...Done.
```

Verifying the configuration

Display files and subdirectories in the root directory of the flash memories on the IRF member devices.

```
<Sysname> dir /all-filesystems
Directory of flash:
   0 -rw-    52922368 Jan 01 2011 08:07:22   5900_r2210.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
```

```
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  11 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (199240 KB free)

Directory of slot2#flash:
   0 -rw-    52922368 Jan 01 2011 08:07:22   5900_r2210.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  11 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (199240 KB free)
```

Configuration files

```
#
 ftp server enable
#
local-user abc class manage
 password hash $h$6$22hpWFZWb0WWfeTp$SSEjRefBG8L0LqgFuO6GwkQTClZe9v9Dykw/MCgbZVF
Eh5yfk4tjEDPnlRbOIQroH4Cyedj7A4P6JWDYkhfxIA==
 service-type ftp
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-admin
#
```

Example: Downloading software from a TFTP server

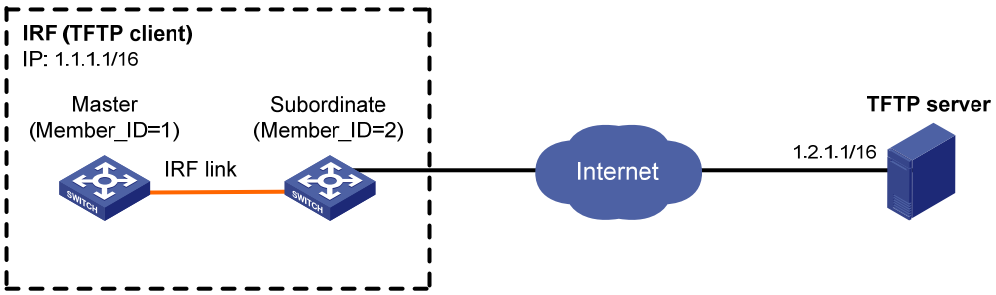
Applicable product matrix

Product series	Software version
HP 5900	Release 2210
HP 5920	Release 2208P01

Network requirements

As shown in Figure 207, use the IRF fabric as a TFTP client to download software images from a TFTP server.

Figure 207 Network diagram



Configuration procedures

This example assumes that the TFTP server and the IRF fabric can ping each other.

Download the file **5900_r2210.ipe** to the root directory of the flash memory on the master switch.

```
<Sysname>tftp 1.2.1.1 get 5900_r2210.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 50.4M  100 50.4M    0     0   143k      0  0:05:59  0:05:59 --:--:-- 93333
```

Download the file **5900_r2210.ipe** to the root directory of the flash memory on the subordinate switch.

```
<Sysname>tftp 1.2.1.1 get 5900_r2210.ipe slot2#flash:/5900_r2210.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 50.4M  100 50.4M    0     0   143k      0  0:05:59  0:05:59 --:--:-- 93333
```

Verifying the configuration

Display files and subdirectories in the root directory of the flash memories on the IRF member devices.

```
<Sysname> dir /all-filesystems
Directory of flash:
   0 -rw-    52922368 Jan 01 2011 08:07:22   5900_r2210.ipe
```

```
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  11 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (199240 KB free)

Directory of slot2#flash:
   0 -rw-    52922368 Jan 01 2011 08:07:22   5900_r2210.ipe
   1 drw-           - Jan 01 2011 00:47:50   core
   2 drw-           - Jan 01 2011 00:00:30   diagfile
   3 -rw-         203 Jan 01 2011 00:24:30   lauth.dat
   4 drw-           - Jan 02 2000 00:00:07   logfile
   5 -rw-    11273216 Jan 01 2011 10:53:44   5900_5920-cmw710-boot-r2208p01
.bin
   6 -rw-    33190912 Jan 01 2011 10:54:49   5900_5920-cmw710-system-r2208p
01.bin
   7 drw-           - Jan 01 2000 00:00:07   seclog
   8 -rw-        3931 Jan 01 2011 00:48:13   startup.cfg
   9 -rw-       78422 Jan 01 2011 00:48:13   startup.mdb
  10 -rw-        3931 Jan 01 2011 00:48:13   startup_bak.cfg
  11 drw-           - Jan 01 2011 04:16:53   versionInfo

524288 KB total (199240 KB free)
```

Configuration files

The system does not save the commands used in this procedure to a configuration file.

Example: Specifying and loading startup software

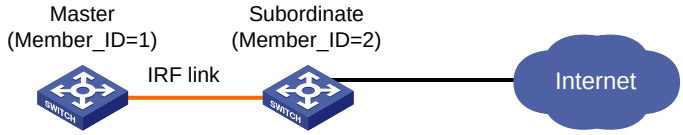
Applicable product matrix

Product series	Software version
HP 5900	Release 2210
HP 5920	Release 2208P01

Network requirements

As shown in Figure 208, the startup software and configuration files are stored on IRF member devices. Use the startup files to upgrade the IRF fabric.

Figure 208 Network diagram



Configuration restrictions and guidelines

All member switches must use the same software image version.

Configuration procedures

Specify **5900_r2210.ipe** as the main startup image file for the master switch.

```
<Sysname>boot-loader file flash:/5900_r2210.ipe slot 1 main
Images in IPE:
  5900_5920-cmw710-boot-r2210.bin
  5900_5920-cmw710-system-r2210.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
The specified file list will be used as the main startup software images at the
next reboot on slot 1.
```

Specify **5900_r2210.ipe** as the main startup image file for the subordinate switch.

```
<Sysname>boot-loader file flash:/5900_r2210.ipe slot 2 main
Images in IPE:
  5900_5920-cmw710-boot-r2210.bin
  5900_5920-cmw710-system-r2210.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
The specified file list will be used as the main startup software images at the
next reboot on slot 2.
```

Reboot the IRF fabric.

```
<Sysname>reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Verifying the configuration

Use the **display version** command to verify that the software has been upgraded.

```
<Sysname> display version
```

```
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P. All rights reserved.
HP 5900-52Q uptime is 0 weeks, 0 days, 2 hours, 18 minutes
Last reboot reason : Power on

Boot image: flash:/5900_5920-cmw710-boot-r2210.bin
Boot image version: 7.1.035P13, Release 2210
System image: flash:/5900_5920-cmw710-system-r2210.bin
System image version: 7.1.035, Release 2210

---- More ----
```

Configuration files

The system does not save the software upgrade commands to configuration files.

Spanning tree configuration examples

This chapter provides spanning tree configuration examples.

General configuration restrictions and guidelines

STP is mutually exclusive with the service loopback function on a port.

Example: Configuring MSTP

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 209:

- Device A and Device B are at the distribution layer.
- Device C, Device D, and Device E are at the access layer.

Configure MSTP to eliminate Layer 2 loops and implement load sharing for redundant links as follows:

- 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 210.

Figure 209 Network diagram

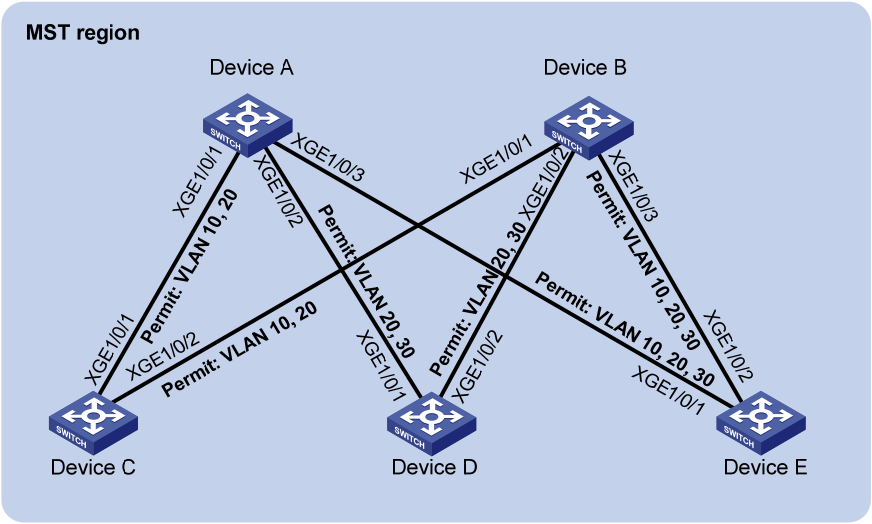
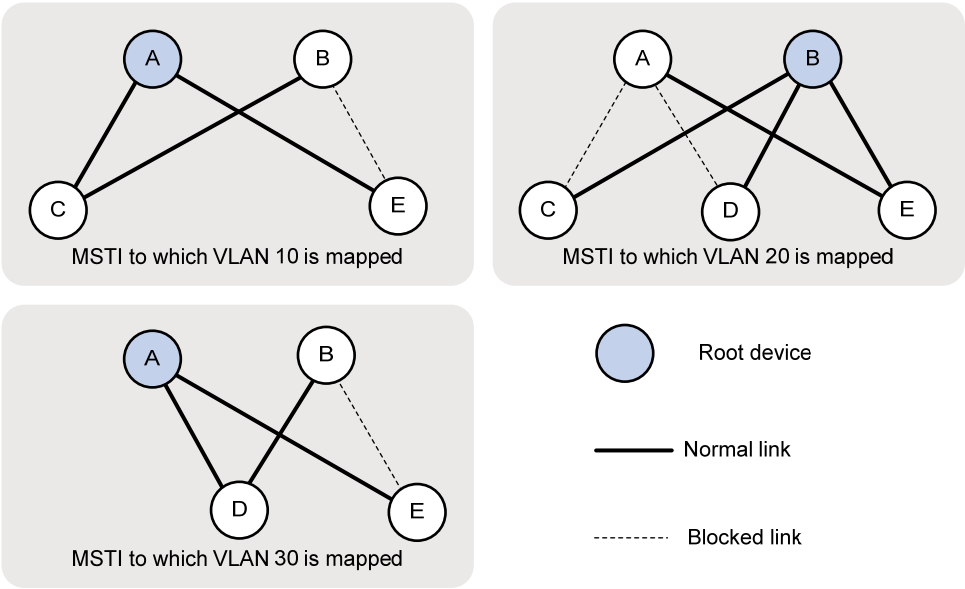


Figure 210 MSTI to which each VLAN is mapped



Requirements analysis

To forward packets from different VLANs along different physical links, set different path costs for a port in different MSTIs. 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.

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.
- HP recommends that you use the **check region-configuration** command to determine whether the MST region configuration to be activated is correct. Activate them only when they are correct.
- The **stp global mcheck** command in system view takes effect on all ports. The **stp mcheck** command in port view takes effect on only the port.

Configuration procedures

In this example, the path cost calculation standard is **legacy** for all devices, and the default path cost of each port is 2.

Configuring VLANs and ports

1. Configure VLANs and ports on Device A:

   # Create VLANs 10, 20, and 30.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] quit
   [DeviceA] vlan 20
   [DeviceA-vlan20] quit
   [DeviceA] vlan 30
   [DeviceA-vlan30] quit
   ```

   # Configure Ten-GigabitEthernet 1/0/1 as a trunk port.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-type trunk
   ```

   # Remove Ten-GigabitEthernet 1/0/1 from VLAN 1.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   ```

   # Assign Ten-GigabitEthernet 1/0/1 to VLANs 10 and 20.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10 20
   ```

   # Enable the spanning tree protocol on Ten-GigabitEthernet 1/0/1. By default, the spanning tree protocol is enabled on a port.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/1] stp enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Configure Ten-GigabitEthernet 1/0/2 as a trunk port.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-type trunk
   ```

   # Remove Ten-GigabitEthernet 1/0/2 from VLAN 1.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
   ```

   # Assign Ten-GigabitEthernet 1/0/2 to VLANs 20 and 30.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 20 30
   ```

   # Enable the spanning tree protocol on Ten-GigabitEthernet 1/0/2. By default, the spanning tree protocol is enabled on a port.

```
[DeviceA-Ten-GigabitEthernet1/0/2] stp enable
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

Configure Ten-GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
```

Remove Ten-GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceA-Ten-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign Ten-GigabitEthernet 1/0/3 to VLANs 10, 20, and 30.

```
[DeviceA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10 20 30
```

Enable the spanning tree protocol on Ten-GigabitEthernet 1/0/3. By default, the spanning tree protocol is enabled on a port.

```
[DeviceA-Ten-GigabitEthernet1/0/3] stp enable
[DeviceA-Ten-GigabitEthernet1/0/3] quit
```

2. Configure VLANs and ports and Device B, Device C, Device D, and Device E in a similar way Device A is configured:
   - Configure VLANs 10, 20, and 30 on Device B and Device E.
   - Configure VLANs 10 and 20 on Device C.
   - Configure VLANs 20 and 30 on Device D.

Configuring Device A

1. Configure the MST region:

   # Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.

   ```
   <DeviceA> system-view
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] region-name example
   ```

   # 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.

   ```
   [DeviceA-mst-region] instance 1 vlan 10
   [DeviceA-mst-region] instance 0 vlan 20
   [DeviceA-mst-region] instance 2 vlan 30
   ```

   # Set the revision level to 0 for the MST region. By default, the revision level is 0.

   ```
   [DeviceA-mst-region] revision-level 0
   ```

2. Verify that the MST region configuration to be activated is correct.

   ```
   [DeviceA-mst-region] check region-configuration
   ```

3. Activate the MST region configuration.

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

4. 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
   ```

5. Configure Device A as a secondary root bridge of MSTI 0.

   ```
   [DeviceA] stp instance 0 root secondary
   ```

6. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

   ```
   [DeviceA] stp mode mstp
   ```

7. Enable the spanning tree protocol globally.

```
[DeviceA] stp global enable
```

8. Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.

```
[DeviceA] stp global mcheck
```

Configuring Device B

1. Configure the MST region:

   # Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.

```
<DeviceB> system-view
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
```

   # 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.

```
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 0 vlan 20
[DeviceB-mst-region] instance 2 vlan 30
```

   # Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
[DeviceB-mst-region] revision-level 0
```

2. Verify that the MST region configuration to be activated is correct.

```
[DeviceB-mst-region] check region-configuration
```

3. Activate the MST region configuration.

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

4. Configure Device B as the primary root bridge of MSTI 0.

```
[DeviceB] stp instance 0 root primary
```

5. 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
```

6. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceB] stp mode mstp
```

7. Enable the spanning tree protocol globally.

```
[DeviceB] stp global enable
```

8. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceB] stp global mcheck
```

Configuring Device C

1. Configure the MST region:

   # Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
```

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.

```
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 0 vlan 20
[DeviceC-mst-region] instance 2 vlan 30
```

Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
[DeviceC-mst-region] revision-level 0
```

2. Verify that the MST region configuration to be activated is correct. Activate them only when they are correct.

```
[DeviceC-mst-region] check region-configuration
```

3. Activate the MST region configuration if the configurations are correct.

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

4. Set the path cost of port Ten-GigabitEthernet 1/0/1 in MSTI 1 to 1.

```
[DeviceC] interface ten-gigabitethernet 1/0/1
[DeviceC-Ten-GigabitEthernet1/0/1] stp instance 1 cost 1
[DeviceC-Ten-GigabitEthernet1/0/1] quit
```

5. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceC] stp mode mstp
```

6. Enable the spanning tree protocol globally.

```
[DeviceC] stp global enable
```

7. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceC] stp global mcheck
```

Configuring Device D

1. Configure the MST region:

Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
```

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.

```
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 0 vlan 20
[DeviceD-mst-region] instance 2 vlan 30
```

Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
[DeviceD-mst-region] revision-level 0
```

2. Verify that the MST region configuration to be activated is correct.

```
[DeviceD-mst-region] check region-configuration
```

3. Activate the MST region configurations if the configurations are correct.

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

4. Set the path cost of port Ten-GigabitEthernet 1/0/1 in MSTI 2 to 1.

```
[DeviceD] interface ten-gigabitethernet 1/0/1
[DeviceD-Ten-GigabitEthernet1/0/1] stp instance 2 cost 1
[DeviceD-Ten-GigabitEthernet1/0/1] quit
```

5. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceD] stp mode mstp
```

6. Enable the spanning tree protocol globally.

```
[DeviceD] stp global enable
```

7. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceD] stp global mcheck
```

Configuring Device E

1. Configure the MST region:

   # Configure the MST region name as **example**. By default, the MST region name is the bridge MAC address of the device.

```
<DeviceE> system-view
[DeviceE] stp region-configuration
[DeviceE-mst-region] region-name example
```

   # 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.

```
[DeviceE-mst-region] instance 1 vlan 10
[DeviceE-mst-region] instance 0 vlan 20
[DeviceE-mst-region] instance 2 vlan 30
```

   # Set the revision level to 0 for the MST region. By default, the revision level is 0.

```
[DeviceE-mst-region] revision-level 0
```

2. Verify that the MST region configuration to be activated is correct.

```
[DeviceE-mst-region] check region-configuration
```

3. Activate the MST region configuration.

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

4. Set the path cost of port Ten-GigabitEthernet 1/0/2 of Device E in MSTI 0 to 1.

```
[DeviceE] interface ten-gigabitethernet 1/0/2
[DeviceE-Ten-GigabitEthernet1/0/2] stp instance 0 cost 1
[DeviceE-Ten-GigabitEthernet1/0/2] quit
```

5. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

```
[DeviceE] stp mode mstp
```

6. Enable the spanning tree protocol globally.

```
[DeviceE] stp global enable
```

7. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceE] stp global 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
 MST ID     Port                              Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1          ALTE  DISCARDING    NONE
   0        Ten-GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
   0        Ten-GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/1          DESI  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/3          DESI  FORWARDING    NONE
   2        Ten-GigabitEthernet1/0/2          DESI  FORWARDING    NONE
   2        Ten-GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID     Port                              Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1          DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2          DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/3          DESI  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/3          ALTE  DISCARDING    NONE
   2        Ten-GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
   2        Ten-GigabitEthernet1/0/3          ALTE  DISCARDING    NONE
```

Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
 MST ID     Port                              Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1          DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/2          DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device D.

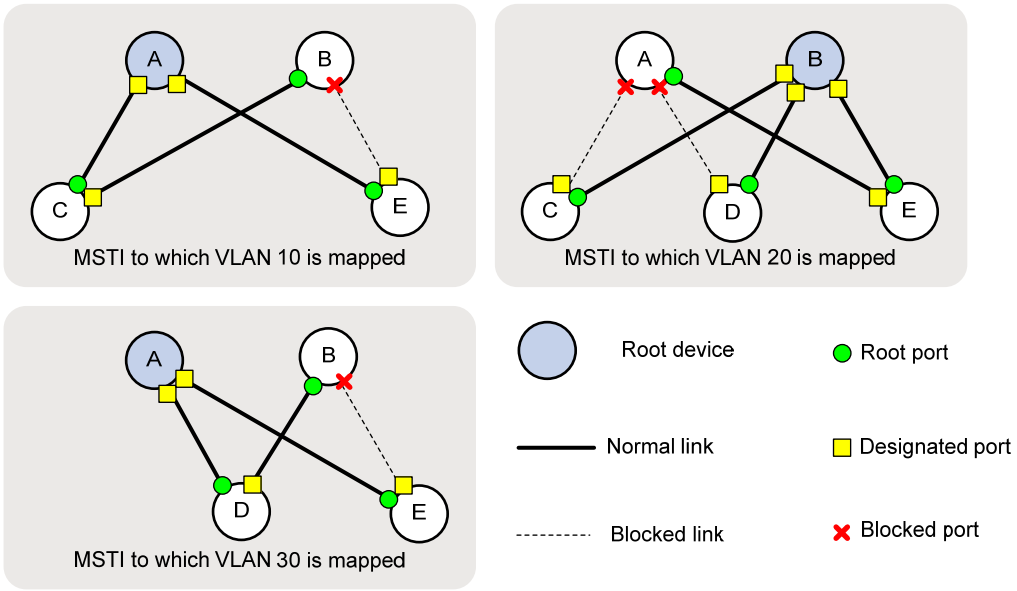
```
[DeviceD] display stp brief
 MST ID     Port                              Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1          DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
   2        Ten-GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
   2        Ten-GigabitEthernet1/0/2          DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device E.

```
[DeviceE] display stp brief
 MST ID     Port                              Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1          DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
   1        Ten-GigabitEthernet1/0/2          DESI  FORWARDING    NONE
   2        Ten-GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
   2        Ten-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 211. The figure shows that the configuration meets the network requirements.

Figure 211 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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 20 30
#
interface Ten-GigabitEthernet1/0/3
 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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
interface Ten-GigabitEthernet1/0/3
  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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 stp instance 1 cost 1
#
interface Ten-GigabitEthernet1/0/2
 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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 stp instance 2 cost 1
#
interface Ten-GigabitEthernet1/0/2
 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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
 stp instance 0 cost 1
#
```

Example: Configuring RSTP

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 212, the LAN has multiple layers:

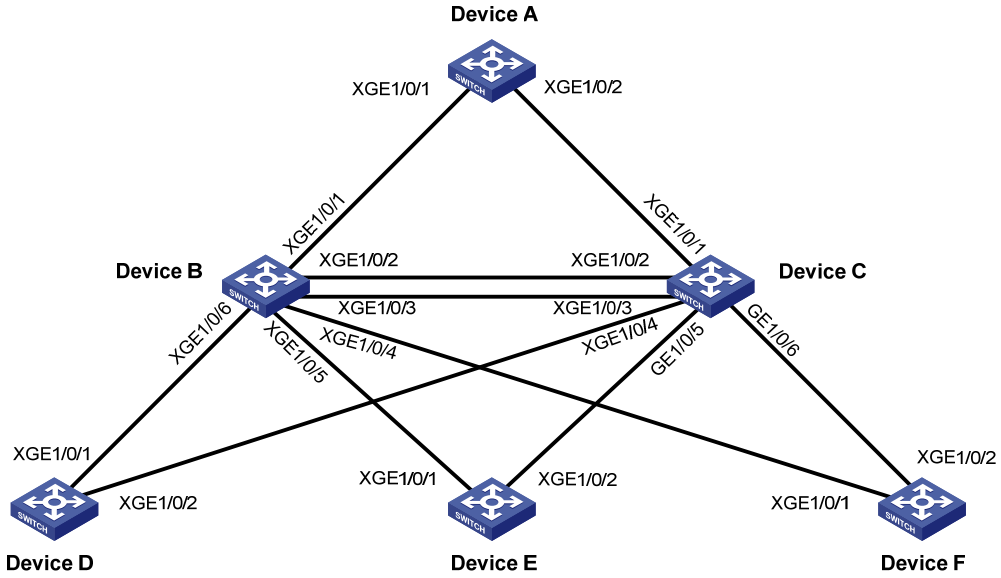
- Device A operates at the core layer.
- Device B and Device C operate at the distribution layer. Device C and Device B are connected through two links.
- Device D, Device E, and Device F operate at the access layer. PCs are directly connected to Device D, Device E, and Device F.
- All ports of these devices have the same path cost.

Configure RSTP to meet the following requirements:

- Device A is the root bridge. Device A is protected against configuration errors and malicious attacks.
- Device C backs up Device B. When Device B fails, Device C takes over to forward data traffic.

- The ports of Device D, Device E, and Device F that directly connect to users are edge ports and have BPDU guard enabled.
- The network is stable and protected against forged TC-BPDUs.

Figure 212 Network diagram



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 restrictions and guidelines

When you configure RSTP, follow these restrictions and guidelines:

- You can configure a device as the primary root bridge by using the **stp root primary** command or by setting the device priority to 0 by using the **stp priority 0** command.
- 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.

Configuration procedures

The following sections describe only the RSTP configurations.

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
```

Enable root guard on the ports connecting Device A to Device B and Device C.

```
[DeviceA] interface Ten-GigabitEthernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] stp root-protection
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface Ten-GigabitEthernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] stp root-protection
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

Enable TC-BPDU guard on Device A. TC-BPDU guard is enabled by default.

```
[DeviceA] stp tc-protection
```

Enable RSTP globally.

```
[DeviceA] stp global enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceA] stp global mcheck
```

Disable STP on the ports that do not participate in the RSTP calculation. This examples uses Ten-GigabitEthernet 1/0/4.

```
[DeviceA] interface Ten-GigabitEthernet 1/0/4
[DeviceA-Ten-GigabitEthernet1/0/4] undo stp enable
[DeviceA-Ten-GigabitEthernet1/0/4] 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 Ten-GigabitEthernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] stp root-protection
[DeviceB-Ten-GigabitEthernet1/0/4] quit
[DeviceB] interface Ten-GigabitEthernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] stp root-protection
[DeviceB-Ten-GigabitEthernet1/0/5] quit
[DeviceB] interface Ten-GigabitEthernet 1/0/6
[DeviceB-Ten-GigabitEthernet1/0/6] stp root-protection
[DeviceB-Ten-GigabitEthernet1/0/6] quit
```

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.

```
[DeviceB] stp global enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceB] stp global mcheck
```

Disable STP on the ports that do not participate in the RSTP calculation. This example uses Ten-GigabitEthernet 1/0/8.

```
[DeviceB] interface Ten-GigabitEthernet 1/0/8
[DeviceB-Ten-GigabitEthernet1/0/8] undo stp enable
[DeviceB-Ten-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 Ten-GigabitEthernet 1/0/4
[DeviceC-Ten-GigabitEthernet1/0/4] stp root-protection
[DeviceC-Ten-GigabitEthernet1/0/4] quit
[DeviceC] interface Ten-GigabitEthernet 1/0/5
[DeviceC-Ten-GigabitEthernet1/0/5] stp root-protection
[DeviceC-Ten-GigabitEthernet1/0/5] quit
[DeviceC] interface Ten-GigabitEthernet 1/0/6
[DeviceC-Ten-GigabitEthernet1/0/6] stp root-protection
[DeviceC-Ten-GigabitEthernet1/0/6] quit
```

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.

```
[DeviceC] stp global enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceC] stp global mcheck
```

Disable STP on the ports that do not participate in the RSTP calculation. This example uses Ten-GigabitEthernet 1/0/8.

```
[DeviceC] interface Ten-GigabitEthernet 1/0/8
[DeviceC-Ten-GigabitEthernet1/0/8] undo stp enable
[DeviceC-Ten-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 Ten-GigabitEthernet 1/0/4.)

```
[DeviceD] interface Ten-GigabitEthernet 1/0/4
[DeviceD-Ten-GigabitEthernet1/0/4] stp edged-port
[DeviceD-Ten-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 global enable
```

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceD] stp global mcheck
```

Disable STP on the ports that do not participate in the RSTP calculation. This example uses Ten-GigabitEthernet 1/0/3.

```
[DeviceD] interface Ten-GigabitEthernet 1/0/3
[DeviceD-Ten-GigabitEthernet1/0/3] undo stp enable
[DeviceD-Ten-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.

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 MST ID     Port                            Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1        DESI  FORWARDING    ROOT
   0        Ten-GigabitEthernet1/0/2        DESI  FORWARDING    ROOT
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID     Port                            Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2        DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/3        DESI  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/4        DESI  FORWARDING    ROOT
   0        Ten-GigabitEthernet1/0/5        DESI  FORWARDING    ROOT
   0        Ten-GigabitEthernet1/0/6        DESI  FORWARDING    ROOT
```

Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
 MST ID     Port                             Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
   0        Ten-GigabitEthernet1/0/3        ALTE  DISCARDING    NONE
   0        Ten-GigabitEthernet1/0/4        DESI  FORWARDING    ROOT
   0        Ten-GigabitEthernet1/0/5        DESI  FORWARDING    ROOT
   0        Ten-GigabitEthernet1/0/6        DESI  FORWARDING    ROOT
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 MST ID     Port                            Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
   0        Ten-GigabitEthernet1/0/4        DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device E.

```
[DeviceE] display stp brief
```

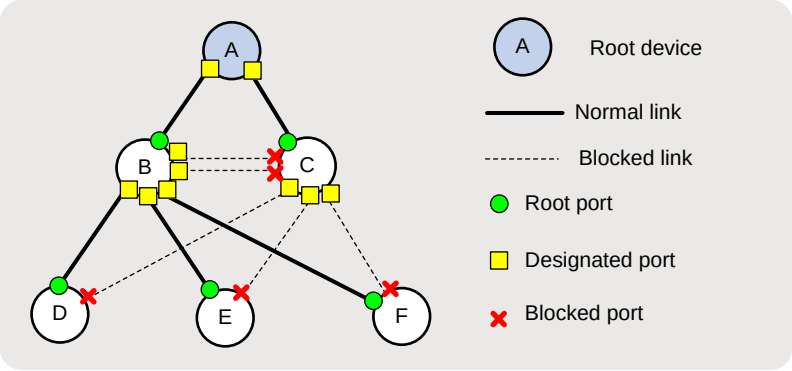
```
MST ID     Port                          Role  STP State     Protection
  0        Ten-GigabitEthernet1/0/1      ROOT  FORWARDING    NONE
  0        Ten-GigabitEthernet1/0/2      ALTE  DISCARDING    NONE
  0        Ten-GigabitEthernet1/0/4      DESI  FORWARDING    NONE
```

Display brief spanning tree information on Device F.

```
[DeviceF] display stp brief
MST ID     Port                          Role  STP State     Protection
  0        Ten-GigabitEthernet1/0/1      ROOT  FORWARDING    NONE
  0        Ten-GigabitEthernet1/0/2      ALTE  DISCARDING    NONE
  0        Ten-GigabitEthernet1/0/4      DESI  FORWARDING    NONE
```

Based on the output, you can draw the topology when the network is stable, as shown in Figure 213.

Figure 213 Network topology



Configuration files

- Device A:

```
#
 stp mode rstp
 stp instance 0 root primary
 stp global enable
#
interface Ten-GigabitEthernet1/0/1
 stp root-protection
#
interface Ten-GigabitEthernet1/0/2
 stp root-protection
#
interface GigabitEthernet1/0/4
 undo stp enable
#
```

- Device B:

```
#
 stp mode rstp
 stp instance 0 priority 4096
 stp global enable
```

```
#
interface Ten-GigabitEthernet1/0/4
 stp root-protection
#
interface Ten-GigabitEthernet1/0/5
 stp root-protection
#
interface Ten-GigabitEthernet1/0/6
 stp root-protection
#
interface Ten-GigabitEthernet1/0/8
 undo stp enable
#
```

- Device C:

```
#
 stp mode rstp
 stp instance 0 priority 8192
 stp global enable
#
interface Ten-GigabitEthernet1/0/4
 stp root-protection
#
interface Ten-GigabitEthernet1/0/5
 stp root-protection
#
interface Ten-GigabitEthernet1/0/6
 stp root-protection
#
interface Ten-GigabitEthernet1/0/8
 undo stp enable
#
```

- Device D:

```
#
 stp mode rstp
 stp bpdu-protection
 stp global enable
#
interface Ten-GigabitEthernet1/0/3
 undo stp enable
#
interface Ten-GigabitEthernet1/0/4
 stp edged-port
#
```

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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

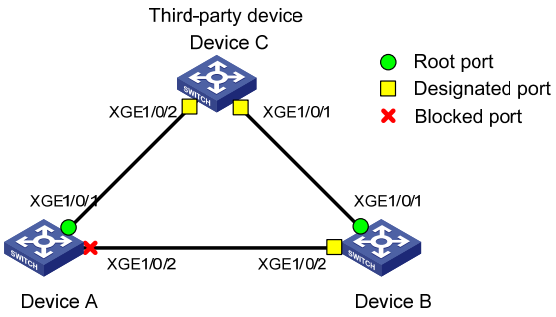
The configuration digest is 16 bytes and is the result calculated by using the HMAC-MD5 algorithm based on VLAN-to-instance mappings. Because spanning tree implementations vary with vendors, the configuration digests calculated through private keys are different. As a result, devices from different vendors in the same MST region cannot communicate with each other.

As shown in Figure 214:

- Device A, Device B, and Device C are interconnected, and they are in the same MST region.
- Device C at MAC address 00e0-fc0e-6554 is a third-party device configured as the root bridge. It uses a private key to calculate the configuration digest.
- The MAC address of Device B is lower than that of Device A.

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 214 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 working correctly.

- 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. This 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.
- 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.

Configuration procedures

Configuring MSTP on Device A

1. Configure the MST region:

   # Configure the MST region name as **example**.

   ```
   <DeviceA> system-view
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] region-name example
   ```

   # Use the default VLAN-to-instance mapping. 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-mst-region] revision-level 0
   ```

2. Verify that the MST region configuration to be activated is correct.

   ```
   [DeviceA-mst-region] check region-configuration
   ```

3. Activate the MST region configuration.

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

4. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

   ```
   [DeviceA] stp mode mstp
   ```

5. Enable the spanning tree protocol globally.

   ```
   [DeviceA] stp global enable
   ```

6. Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.

   ```
   [DeviceA] stp global mcheck
   ```

Configuring MSTP on Device B

Configure MSTP on Device B in the same way MSTP is configured on Device A.

Configuring MSTP on Device C (the third-party device)

Configure MSTP on Device C as follows:

- Configure the MST region name as **example**.
- Map VLANs 1 through 4094 to instance 1.
- Set the revision level to 0 for the MST region.
- Verify that the MST region configurations are correct.
- Configure Device C as the root bridge of instance 0.

- Enable the spanning tree protocol.

For information about configuring MSTP on Device C, see the configuration guide for Device C.

Configuring digest snooping on Device A

Enable digest snooping on port Ten-GigabitEthernet 1/0/1.

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

Enable digest snooping globally.

```
[DeviceA] stp global config-digest-snooping
```

Configuring digest snooping on Device B

Enable digest snooping on port Ten-GigabitEthernet 1/0/1.

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

Enable digest snooping globally.

```
[DeviceB] stp global config-digest-snooping
```

Verifying the configuration

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 MST ID     Port                           Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1       ROOT  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2       ALTE  DISCARDING    NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID     Port                           Role  STP State     Protection
   0        Ten-GigabitEthernet1/0/1       ROOT  FORWARDING    NONE
   0        Ten-GigabitEthernet1/0/2       DESI  FORWARDING    NONE
```

Display the root bridge of HP devices, for example, Device A.

```
<DeviceA> display stp root
 MST ID Root Bridge ID        ExtPathCost  IntPathCost Root Port
   0    0.00e0-fc0e-6554      20           0           Ten-GigabitEthernet1/0/1
```

The output shows that:

- The root bridge of Device A is Device C.
- Device A, Device B, and Device C can communicate with each other in the same region.

Configuration files

- Device A:

```
#
```

```
stp region-configuration
 region-name example
 active region-configuration
#
 stp global enable
#
 stp global config-digest-snooping
#
interface Ten-GigabitEthernet1/0/1
 stp config-digest-snooping
#
```

- Device B:

```
#
stp region-configuration
 region-name example
 active region-configuration
#
 stp global enable
#
 stp global config-digest-snooping
#
interface Ten-GigabitEthernet1/0/1
 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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

The designated port of an RSTP or MSTP device can implement rapid state transition through exchanging Proposal and Agreement packets with the root port of a downstream device.

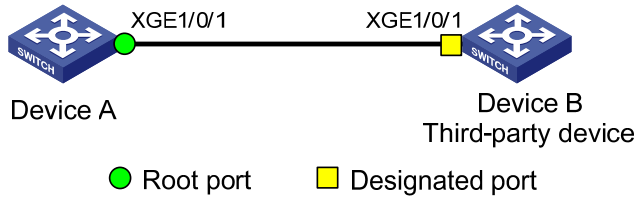
When the downstream device is an HP device and is connected to a third-party upstream device that has a private spanning tree implementation, the rapid state transition implementation might be limited.

As shown in Figure 215:

- 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 Ten-GigabitEthernet 1/0/1 on Device B can rapidly transit its port state.

Figure 215 Network diagram



Configuration restrictions and guidelines

When you configure No Agreement Check, follow these restrictions and guidelines:

- To make the No Agreement Check feature take effect, enable the feature on the root port.
- 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.

Configuration procedures

Configuring MSTP on Device A

1. Configure the MST region:

   # Configure the MST region name as **example**.

   ```
   <DeviceA> system-view
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] region-name example
   ```

   # Use the default VLAN-to-instance mapping. 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-mst-region] revision-level 0
   ```

2. Verify that the MST region configuration to be activated is correct.

   ```
   [DeviceA-mst-region] check region-configuration
   ```

3. Activate the MST region configuration.

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

4. Set the spanning tree mode to MSTP. By default, the spanning tree mode is MSTP.

   ```
   [DeviceA] stp mode mstp
   ```

5. Enable the spanning tree protocol globally.

   ```
   [DeviceA] stp global enable
   ```

6. Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.

```
[DeviceA] stp global mcheck
```

Configuring MSTP on Device B (the third-party device)

Configure MSTP on Device B as follows:

- Configure the MST region name as **example**.
- Map VLANs 1 through 4094 to instance 1.
- Set the revision level to 0 for the MST region.
- Verify that the MST region configurations are correct.
- Configure Device B as the root bridge of instance 0.
- Enable the spanning tree protocol.

For information about configuring MSTP on Device B, see the configuration guide for Device B.

Configuring No Agreement Check on Device A

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

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

Verifying the configuration

Connect Device A to Device B. Then, immediately execute the **display stp brief** command multiple times to display the brief spanning tree information on Device B.

The output shows that the designated port GigabitEthernet 1/0/1 rapidly transits to the forwarding state in 2 to 3 seconds.

Configuration files

Device A:

```
#
stp region-configuration
 region-name example
 active region-configuration
#
 stp global enable
#
interface Ten-GigabitEthernet1/0/1
 stp no-agreement-check
#
```

SSH configuration examples

This chapter provides examples for configuring SSH for secure remote access and file transfer.

The switches in the configuration examples are operating in non-FIPS mode.

General configuration restrictions and guidelines

When you configure SSH, follow these restrictions and guidelines:

- When acting as an SSH server, the switch supports SSH2 and SSH1 in non-FIPS mode and supports only SSH2 in FIPS mode. When acting as an SSH client, the switch supports SSH2.0 only.
- Do not generate the local DSA key pair when the device operates in FIPS mode as an SSH server. User authentication will fail because the SSH server operating in FIPS mode supports only RSA key pairs.

Example: Configuring the switch as an Stelnet server for password authentication

Applicable product matrix

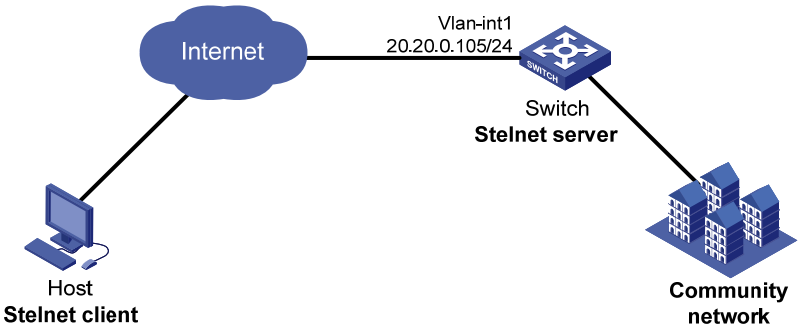
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 216, 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. It uses local password authentication.
- The switch limits the number of authentication attempts to prevent malicious hacking of usernames and passwords.

Figure 216 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 ensure login of SSH clients that use different types of key pairs, generate both DSA and RSA key pairs on the SSH server.
- The user role for the password authenticated Stelnet user is obtained by using one of the following methods:
  - Authorized by the AAA server.
  - Specified by the **authorization-attribute** command in the associated local user view.
- 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 on only the users at the 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 key pairs.

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:2048
Generating Keys...
..................+++
.....................................................................................
```

```
..........+++
......++++++++
............++++++++
Create the key pair successfully.
```

Generate a DSA key pair.

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:2048
Generating Keys...
...+.....................+..........+...................+.+......+.+.......+...
.............................................++++++++++++++++++++++++++++++++++
++++++++++++++++*
........+........+............+..+..+..+.+..................+.......+.......+...
.......+...+.......+...+..+..................+...........+.+..............+....+
.........+......................+.........+........+.......+.+..................+
.........+.....+............+..+.....................................+..........
+....+...........+.+....+.+..........+..........+............+..................
...........+..+....+........+.......+..........+....+..............+.+.+........
.............+........+......+.+......................+.......+..................
.....+.......................+.........+.............+.....+..+..................
.........+........+..+..........+.......+.....++++++++++++++++++++++++++++++++
++++++++++++++++*
Create the key pair successfully.
```

Enable the SSH server function.

```
[Switch] ssh server enable
```

Set the maximum number of SSH authentication attempts to 5.

```
[Switch] ssh server authentication-retries 5
```

Set the authentication mode to AAA for the user interfaces.

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

Create a local device management user **client001** with the password **aabbcc**, the service type **ssh**, and the user role **network-admin**.

```
[Switch] local-user client001 class manage
New local user added.
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
```

Delete the default user role **network-operator** for the user, so that only the authorized user role **network-admin** is available for the user.

```
[Switch-luser-manage-client001] undo authorization-attribute user-role network-operator
[Switch-luser-manage-client001] quit
```

Create an SSH user **client001**. Specify the service type for the user as **Stelnet** and the authentication method as **password**. By default, password authentication is used if an SSH user is not created.

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

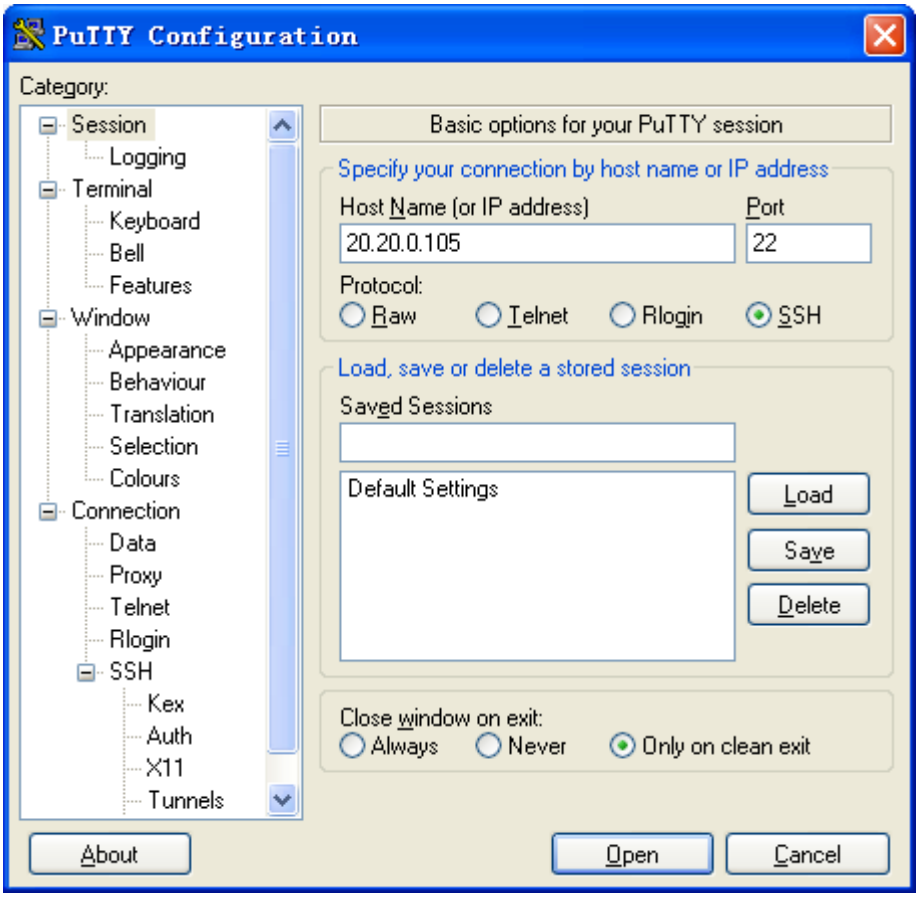
Configuring the SSH client

There are different types of Stelnet client software, including 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 to enter the interface shown in Figure 217.
2. In the **Host Name (or IP address)** field, enter the IP address **20.20.0.105** of the Stelnet server.

Figure 217 Specifying the Stelnet server



3. Click **Open**.

   A security alert dialog box appears to ask you 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
#
interface Vlan-interface1
 ip address 20.20.0.105 255.255.255.0
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
 ssh server authentication-retries 5
 ssh user client001 service-type stelnet authentication-type password
#
local-user client001 class manage
 password hash $h$6$mSlOltEn0kBbM3bT$CxfeBuwEl3ffZIP0MRqK5sh7P9/v4DPoyNsoXhriVVU
NG6eG+AIMM8M170pRPPnOwq2AN+AXpvby8blYvN5FHg==
 service-type ssh
 authorization-attribute user-role network-admin
#
```

Example: Configuring the switch as an Stelnet server for publickey authentication

Applicable product matrix

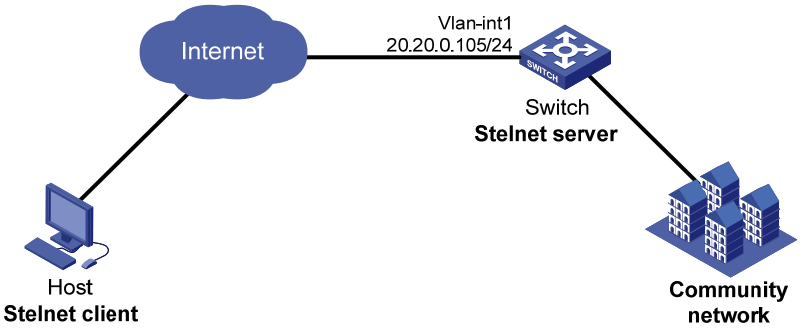
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 218, 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 218 Network diagram



Requirements analysis

For successful publickey authentication, you must perform the following tasks:

1. Generate RSA key pairs on the client.
2. Upload the client's host public key to the server.
3. 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

The user role for the publickey authenticated Stelnet user is specified by the **authorization-attribute** command in the associated local user view.

Configuration procedures

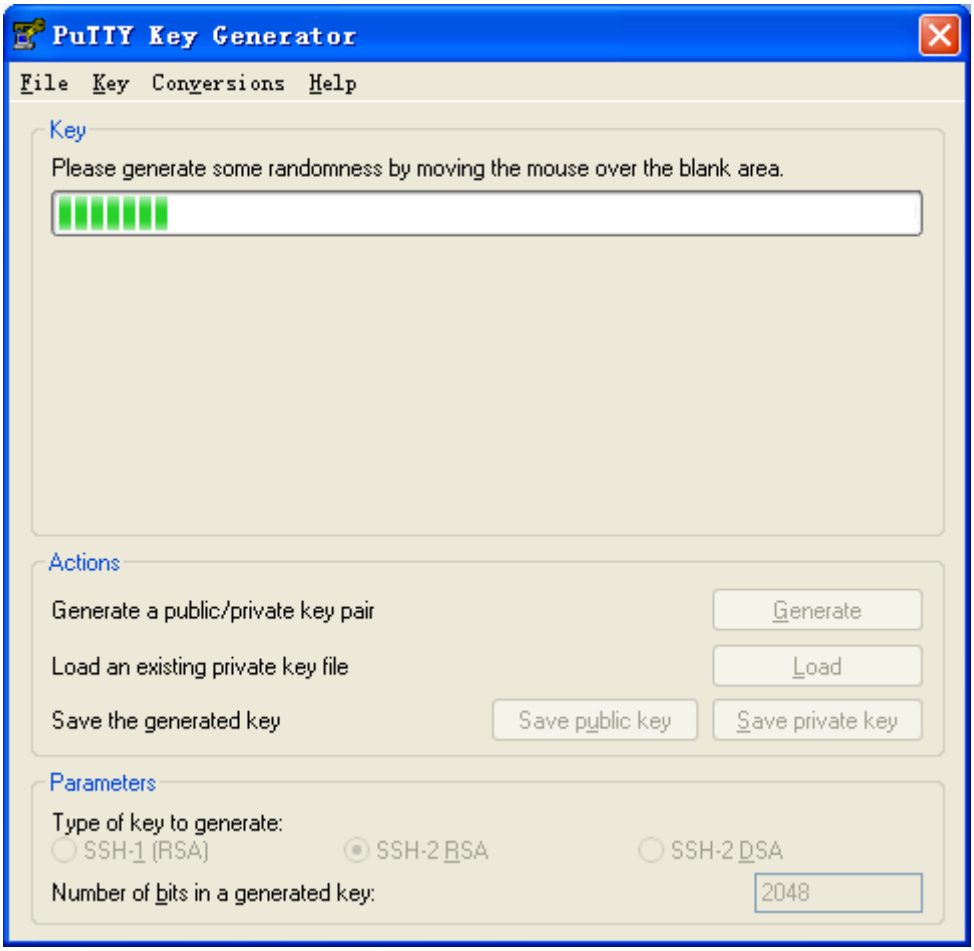
Configuring the Stelnet client

1. Run PuTTYGen.exe on the client to enter the interface shown in Figure 219.
2. Select **SSH-2 RSA** and enter **2048** in the **Number of bits in a generated key** field.
3. Click **Generate**.

Figure 219 Generating the RSA key pairs on the client

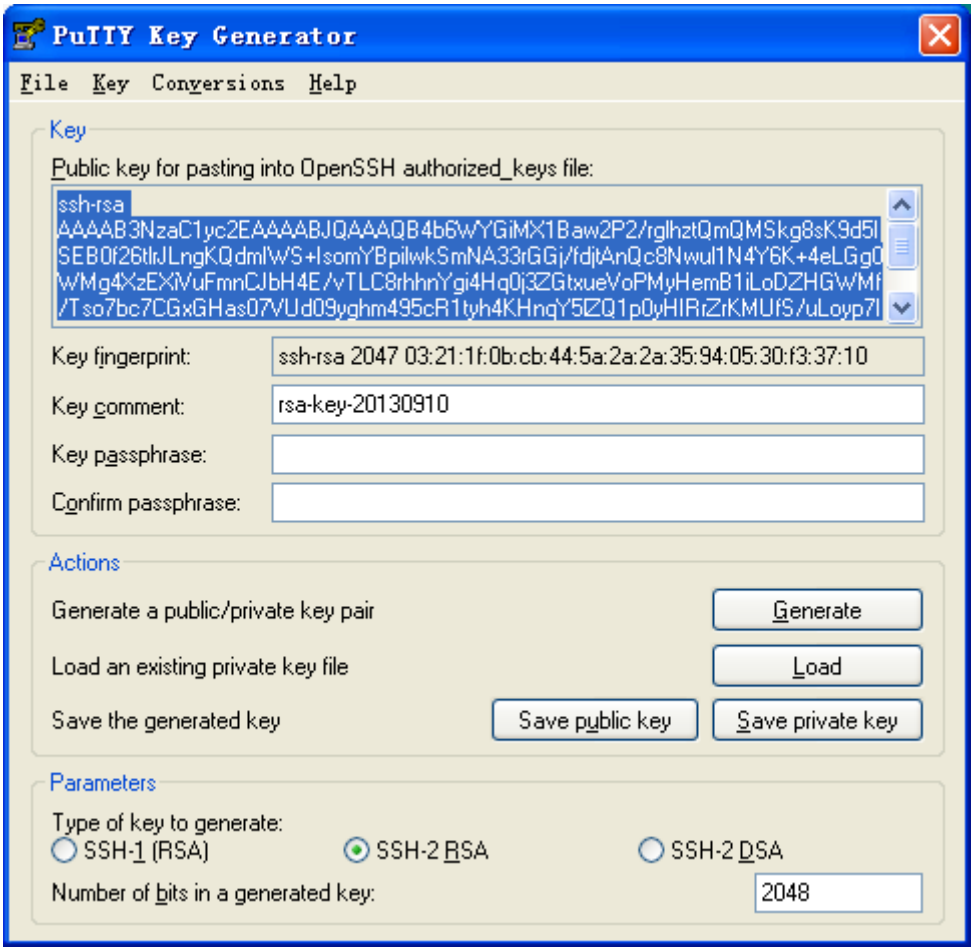
4. Continuously move the mouse and do not place the mouse over the progress bar shown in Figure 220. Otherwise, the key pair generating progress stops.

Figure 220 Generating process



5. Save the public key after the key pair is generated:
   a. Click **Save public key**.
      A file saving window appears.
   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 221 Saving the generated key pair



6. Click **Save private key** to save the private key.

   A confirmation dialog box appears.
7. Click **Yes**.

   A file saving window appears.
8. Specify a directory (root directory of disk C in this example).
9. Enter a file name (**private.ppk** in this example)
10. 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**, the user role **network-admin**, and the working directory **flash:/**.

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

```
[Switch-luser-manage-ftp] password simple ftp
[Switch-luser-manage-ftp] authorization-attribute user-role network-admin
[Switch-luser-manage-ftp] authorization-attribute work-directory flash:/
[Switch-luser-manage-ftp] service-type ftp
[Switch-luser-manage-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 successful.
150 Connecting to port 5001
226 File successfully transferred
ftp> bye
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.

c:\
```

Configuring the switch as an Stelnet server

Generate the RSA key pairs.

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

Enable the SSH server function.

```
[Switch] ssh server enable
```

Set the authentication mode to AAA for the user interfaces.

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

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
```

Import the client's public key from the file **key.pub** and name it **Switch001**.

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

Create a local device management user **client002** with the service type **ssh** and the user role **network-admin**.

```
[Switch] local-user client002 class manage
New local user added.
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

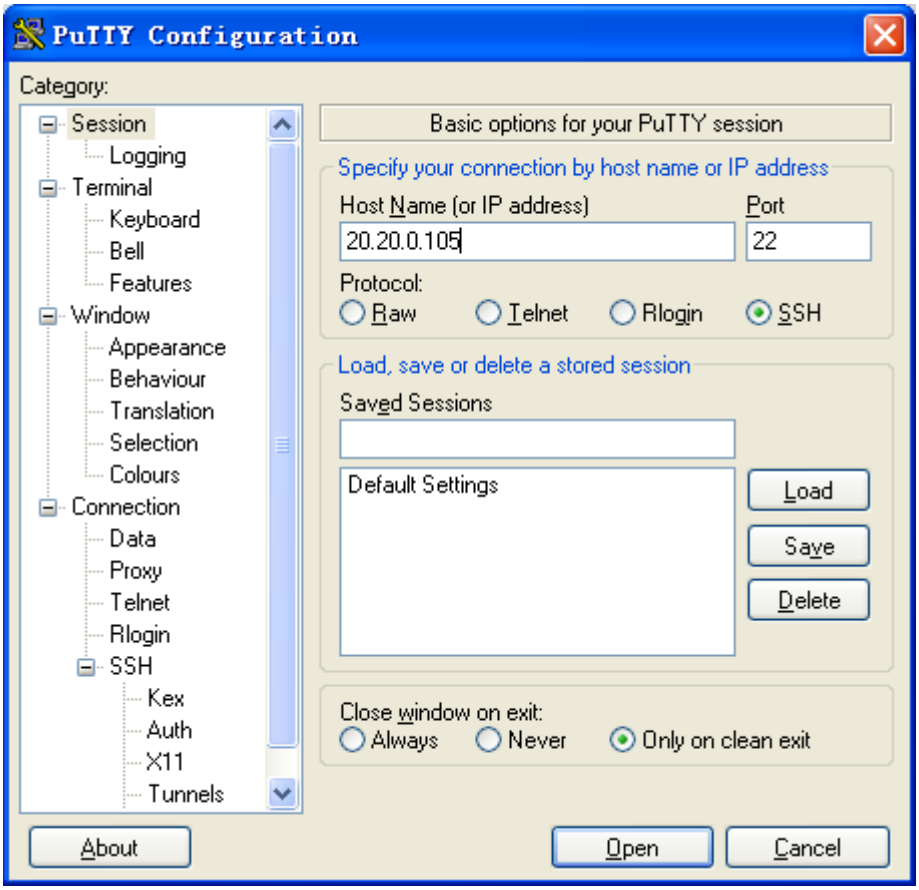
Create an SSH user **client002**. Specify the authentication method as **publickey** for the user and assign the public key **Switch001** to the user.

```
[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 to enter the interface shown in Figure 222.
2. In the **Host Name (or IP address)** field, enter the IP address **20.20.0.105** of the Stelnet server.

Figure 222 Specifying the Stelnet server



3. Select **Connection** > **SSH** > **Auth** from the navigation tree.

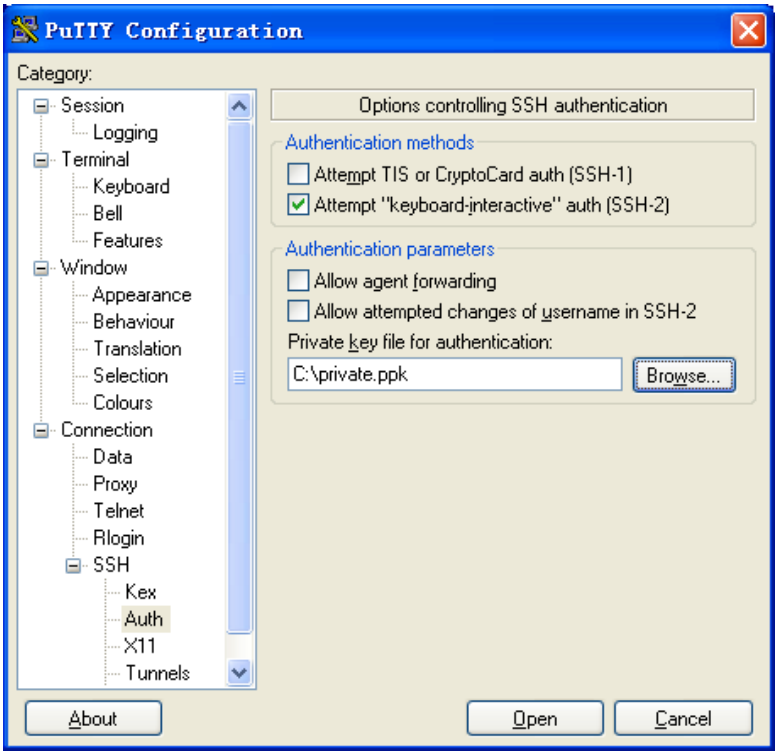
   The window shown in Figure 223 appears.

4. Click **Browse...**.

   A file selection window appears.

5. Select the private key file **private.ppk**, and click **OK**.

   Figure 223 Specifying the private key file



6. Click **Open** to connect to the server.

   A confirmation dialog box appears.

7. Click **Yes**.

8. 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-20130910”

***************************************************************************
* 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

```
#
 ftp server enable
#
vlan 1
#
interface Vlan-interface1
 ip address 20.20.0.105 255.255.255.0
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
 protocol inbound ssh
#
 ssh server enable
 ssh user client002 service-type stelnet authentication-type publickey assign pu
blickey Switch001
#
local-user client002 class manage
 service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
local-user ftp class manage
 password hash $h$6$rPGf1u0xsv3fN3X5$klFjlO31PR0MYz8BNqW1PIE1f+sOdAVeVNEmqa8s6tI
ciDOMelH2/ZGxNwaYMXX5VdnQCs7RU1OAhx0/IpkRWg==
 service-type ftp
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
public-key peer Switch001
 public-key-code begin
   30820120300D06092A864886F70D0101010500038201 0D00308201080282010100D7A2FC65
   000A6CE396F3E3A3FD64AC23C61845864BD377C858952DCCBD63FFA695333B82CB467C928E
   3A7FF9DD6580212514953A4912D72B47FC61709BF2354575D1D68611DC313E81E0E988BCDB
   4A24B003E77031D3D81CD57451B84BEDB706373927AAEFB545FD9CFEC4B38FB0695BD8D18E
   92A10688B60D00537A7F606ECBC5B44228EAAA29E7135103CC8800FF0A825CFAA0DAE3311E
   97D821F1B3007E88B2B3E3BBF50ECD4A7558BEE768B4E08EE764900A8AA60C1DC887DA6288
   C2A7AF62FA5AAEFF806788CE003D48015E7DBBE3B74F93646607A6363D0C0C25C35E3566C6
   8A3B8CEC4B7A47D22F4EDDD36A9C5A630F2A7C638CD37E441EFE28B530F5020125
 public-key-code end
 peer-public-key end
#
```

Example: Configuring the switch as an Stelnet client for password authentication

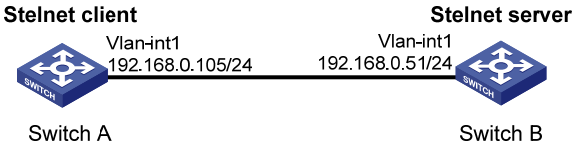
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 224, you can log in to Switch B through the Stelnet client that runs on Switch A. After login, you are assigned the user role **network-admin** for configuration and management. Switch B acts as the Stelnet server and uses password authentication. The username and password of the client are saved on Switch B.

Figure 224 Network diagram



Configuration restrictions and guidelines

When you configure the switch as an Stelnet client for password authentication, follow these restrictions and guidelines:

- When you try to access an Stelnet server, the client must use the server's host public key to authenticate the server. If you have not configured the server's host public key on the client, the client will ask you whether you want to continue with the access.
  - If you choose to continue, the client accesses the server and downloads the server's host public key.
  - If you choose to not continue, the connection cannot be established.

  In an insecure network, HP recommends that you configure the server's host public key on the client.
- The user role for the password authenticated Stelnet user is obtained by using one of the following methods:
  - Authorized by the AAA server.
  - Specified by the **authorization-attribute** command in the associated local user view.

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 modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..........+..........+..........+..+.+.........+......+......+...+..+......
...+..........+..........+.........+.....+................+.+..+..........
......++++++++++++++++++++++++++++++++++++++++++++++++++*
.............+........+.+.+........+..........+.................+...+......
++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Generate RSA key pairs.

```
[SwitchB] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.......+++
.............................................................+++
........++++++++
........++++++++
Create the key pair successfully.
```

Display the DSA key pair on Switch B.

```
[SwitchB ] display public-key local dsa public

=============================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 12:28:38 2013/09/10
Key code:

   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
```

```
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100D383008A4A4A36764A36EAA682E2C0F9EA
   63EA5006DBC94AD4AC680CD25E9C104E682A41EF739BD9378644EF943EEEC3F7C69CB9542D
   747984E61BE40146E932B1FA1301D717C3008E4B9BECBA1C524000598ADC6A5DF97B78BD05
   F6565ECED8EFE2347B36A68EF03C5042981DE1110A13075068635E41385CC271FF1F64C797
```

Display the RSA key pairs on Switch B.

```
[SwitchB] display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 12:28:49 2013/09/10
Key code:

   30819F300D06092A864886F70D010101050003818D0030818902818100D7B0F1A80618954
   6BE57E25528D73CCA4547018B0369DD0AA84B935CFB617179616620FC320CB5F0132328A59
   1E76A8422DA35FA1265120580D6C9911C9F1A1E8AD22F3730683744BA35B7D0F608DC16085
   0036DE792FBE05309F5167542960DBEF47F3A0E6C9C63C4B25418E2877693E49FABA5930CB
   8CE52918D96D6A21E50203010001

=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 12:28:49 2013/09/10
Key code:

   307C300D06092A864886F70D0101010500036B003068026100D971EC82BA09CA96AA30B11A
   F872D83343CA537CFD3E76F04EFB5A4EC2DEDB21E5CE0B1463770F8CC96442CCDF00CB1D15
   B90B21233F88E5630F873B6B45D58D172DE3D271E6B7B888738FD10386A287C7E8E92686CF
   029AE22FD06014EA8DE90203010001
```

Enable the SSH server function.

```
[SwitchB] ssh server enable
```

Set the authentication mode to AAA for the user interfaces.

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

Create a local device management user **client001** with the plaintext password **aabbcc,** the service type **ssh**, and the user role **network-admin**.

```
[SwitchB] local-user client001 class manage
New local user added.
[SwitchB-luser-manage-client001] password simple aabbcc
[SwitchB-luser-manage-client001] service-type ssh
```

```
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
```

Create an SSH user **client001**. Specify the service type for the user as **Stelnet** and the authentication method as **password**. By default, password authentication is used if an SSH user is not created.

```
[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
```

Verifying the configuration

1. Verify that you can access the Stelnet server if you do not configure the server's host public key on the client. When you access the server, the system will ask you whether to continue with the access. Select **Yes** to access the server and download the server's host public key.

   # Establish the connection with the Stelnet server **192.168.0.51**.

   ```
   <SwitchA> ssh2 192.168.0.51
   Username: client001
   The server is not authenticated. Continue? [Y/N]:y
   Do you want to save the server public key? [Y/N]:y
   client001@192.168.0.51'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.                 *
   ***************************************************************************

   <SwitchB>
   ```

   After you enter the correct password, you can successfully log in to the server successfully. At the next connection attempt, the client authenticates the server by using the saved server's host public key on the client.

   # Establish the connection with the Stelnet server **192.168.0.51**.

   ```
   <SwitchA> ssh2 192.168.0.51
   Username: client001
   client001@192.168.0.51'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.                 *
   ***************************************************************************
   ```

```
<SwitchB>
```

2. Verify that you can access the Stelnet server after the host public key of the server is configured on the client:

   # Use the **display public-key local dsa public** command on the server to display the server's host public key.

   # Enter public key view of the client and copy the host public key of the server to the client.

```
[SwitchA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[SwitchA-pkey-public-key-key1]308201B83082012C06072A8648CE3804013082011F02818100
D757262C4584C44C211F18BD
[SwitchA-pkey-public-key-key1]96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE0
8CECE65BE6C265854889DC1E
[SwitchA-pkey-public-key-key1]DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F2
2C3C89CB9B06FD60FE01941D
[SwitchA-pkey-public-key-key1]DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F
358214B16A2FAC4B36895038
[SwitchA-pkey-public-key-key1]7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDA
CE915F0281810082269009E1
[SwitchA-pkey-public-key-key1]4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5
EF93133E84B47093C52B20CD
[SwitchA-pkey-public-key-key1]35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132
CE71B020217091AC717B6123
[SwitchA-pkey-public-key-key1]91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E8105
61C21621C73D6DAAC028F4B1
[SwitchA-pkey-public-key-key1]585DA7F42519718CC9B09EEF038185002818100D383008A4A
4A36764A36EAA682E2C0F9EA
[SwitchA-pkey-public-key-key1]63EA5006DBC94AD4AC680CD25E9C104E682A41EF739BD93786
44EF943EEEC3F7C69CB9542D
[SwitchA-pkey-public-key-key1]747984E61BE40146E932B1FA1301D717C3008E4B9BECBA1C52
4000598ADC6A5DF97B78BD05
[SwitchA-pkey-public-key-key1]F6565ECED8EFE2347B36A68EF03C5042981DE1110A13075068
635E41385CC271FF1F64C797
[SwitchA-pkey-public-key-key1]peer-public-key end
[SwitchA]quit
```

   # Establish the connection to the server **192.168.0.51** and specify the host public key of the server.

```
<SwitchA> ssh2 192.168.0.51 publickey key1
Username: client001
client001@192.168.0.51'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.                    *
******************************************************************************

<SwitchB>
```

   After you enter the correct password, you log in to the server successfully.

Configuration files

- Switch A:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.105 255.255.255.0
#
public-key peer 192.168.0.51
 public-key-code begin
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100D383008A4A4A36764A36EAA682E2C0F9EA
   63EA5006DBC94AD4AC680CD25E9C104E682A41EF739BD9378644EF943EEEC3F7C69CB9542D
   747984E61BE40146E932B1FA1301D717C3008E4B9BECBA1C524000598ADC6A5DF97B78BD05
   F6565ECED8EFE2347B36A68EF03C5042981DE1110A13075068635E41385CC271FF1F64C797
 public-key-code end
 peer-public-key end
#
public-key peer key1
 public-key-code begin
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100D383008A4A4A36764A36EAA682E2C0F9EA
   63EA5006DBC94AD4AC680CD25E9C104E682A41EF739BD9378644EF943EEEC3F7C69CB9542D
   747984E61BE40146E932B1FA1301D717C3008E4B9BECBA1C524000598ADC6A5DF97B78BD05
   F6565ECED8EFE2347B36A68EF03C5042981DE1110A13075068635E41385CC271FF1F64C797
 public-key-code end
 peer-public-key end
#
```

- Switch B:

```
#
vlan 1
#
```

```
interface Vlan-interface1
 ip address 192.168.0.51 255.255.255.0
#
user-interface vty 0 15
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
 ssh user client001 service-type stelnet authentication-type password
#
local-user client001 class manage
 password hash $h$6$JM2d+CjyWo60Lx+z$QN5/eszOsB2t9nULUaEJVrEU4cZl3HNdYx1Gykx2bVk
IqEaxZD8Kh62gN/HHesf8Dnd/1USVMU6MTck2agnk6A==
 service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
```

Example: Configuring the switch as an SFTP client for publickey authentication

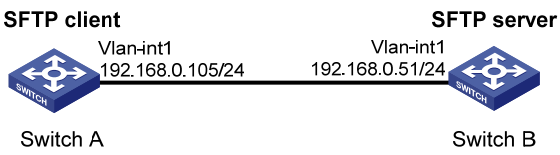
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 225, you can log in to Switch B through the SFTP client that runs on Switch A. After login, you are assigned the user role **network-admin** for file management and transferring operations. Switch B acts as the SFTP server and uses publickey authentication and DSA public key algorithm.

Figure 225 Network diagram



Requirements analysis

For successful publickey authentication, you must perform the following tasks:

1. Generate a DSA key pair on Switch A.
2. Upload the switch's host public key to Switch B.
3. 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 restrictions and guidelines

When you configure the switch as an SFTP client for publickey authentication, follow these restrictions and guidelines:

- When you try to access an SFTP server, the client must use the server's host public key to authenticate the server. If you have not configured the server's host public key on the client, the client will ask you whether you want to continue with the access.
  - If you choose to continue, the client accesses the server and downloads the server's host public key.
  - If you choose to not continue, the connection cannot be established.

  In an insecure network, HP recommends that you configure the server's host public key on the client.
- Both the user role and working directory of the publickey authenticated SFTP user are specified by the **authorization-attribute** command in the associated local user view.

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 modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........+......+...+..+.....................+.............+.........+..+.....
..++++++++++++++++++++++++++++++++++++++++++++++++++*
.......................+....+.............................................+..
...+............+..+......++++++++++++++++++++.
++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

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 with the service type as **ftp** with both the username and password **ftp**, the user role **network-admin**, and the working directory **flash:/**.

```
[SwitchB] local-user ftp class manage
New local user added.
[SwitchB-luser-manage-ftp] password simple ftp
[SwitchB-luser-manage-ftp] authorization-attribute user-role network-admin
[SwitchB-luser-manage-ftp] authorization-attribute work-directory flash:/
[SwitchB-luser-manage-ftp] service-type ftp
[SwitchB-luser-manage-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
Connected to 192.168.0.51 (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.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put key2.pub
227 Entering Passive Mode (192,168,0,51,157,66)
150 Accepted data connection
226 File successfully transferred
677 bytes sent in 0.000381 seconds (1.69 Mbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 0 kbytes.
221 Logout.
```

Configuring Switch B as the SFTP server

Generate a DSA public key pair.

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

```
.........................+..+...........+.......+..................+.......
...+........+.+............++++++++++++++++++++++++++++++++++++++++++++++++*
..........+.....+......+..........+....+.....+..+....+.......+........+.......
....+........+..+..+......+...............+.....+.........+.+.............+.
.+.+.......+..........+....+..+.....+...........................+.........+.
++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Enable the SSH server function

```
[SwitchB] ssh server enable
```

Enable the SFTP server.

```
[SwitchB] sftp server enable
```

Import the peer public key from the file **key2.pub**.

```
[SwitchB] public-key peer Switch001 import sshkey key2.pub
```

Create a local device management user **client002**. Specify the service type as **SSH**, the user role as **network-admin**, and the working directory as **flash:/**.

```
[SwitchB] local-user client002 class manage
New local user added.
[SwitchB-luser-manage-client002] service-type ssh
[SwitchB-luser-manage-client002] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client002] authorization-attribute work-directory flash:/
[SwitchB-luser-manage-client002] quit
```

Create an SSH user **client002**. Specify the service type as **sftp** and authentication method as **publickey** for the user. Assign the public key **Switch001** to the user, and 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

Establish a connection to the SFTP server and enter SFTP client view.

```
<SwitchA> sftp 192.168.0.51 identity-key dsa
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.0.51 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
sftp>
Do you want to save the server public key? [Y/N]:n
```

Display files under the current directory of the server.

```
sftp> dir
-rw-rw-rw-    1 1        1        44890112 Jan  1 06:06 5800.ipe
-rw-rw-rw-    1 1        1        33679360 Jan  1 04:55 5900_5920-cmw710-system-
r2210.bin
-rw-rw-rw-    1 1        1            5427 Jan  1 00:20 basic.cfg
-rwxrwxrwx    1 1        1           94145 Jan  1 00:20 basic.mdb
-rwxrwxrwx    1 1        1             677 Jan  1 01:17 key2.pub
```

```
drwxrwxrwx    1 1        1            2048 Jan  1 00:12 logfile
sftp>
```

Add a directory named **new1** and verify the result.

```
sftp> mkdir new1
sftp> dir
-rw-rw-rw-    1 1        1        44890112 Jan  1 06:06 5800.ipe
-rw-rw-rw-    1 1        1        33679360 Jan  1 04:55 5900_5920-cmw710-system-
r2210.bin
-rw-rw-rw-    1 1        1            5427 Jan  1 00:20 basic.cfg
-rwxrwxrwx    1 1        1           94145 Jan  1 00:20 basic.mdb
-rwxrwxrwx    1 1        1             677 Jan  1 01:17 key2.pub
drwxrwxrwx    1 1        1            2048 Jan  1 00:12 logfile
drwxrwxrwx    1 1        1            2048 Jan  1 01:32 new1
```

Rename directory **new1** to **new2** and verify the result.

```
sftp> rename new1 new2
sftp> dir
-rw-rw-rw-    1 1        1        44890112 Jan  1 06:06 5800.ipe
-rw-rw-rw-    1 1        1        33679360 Jan  1 04:55 5900_5920-cmw710-system-
r2210.bin
-rw-rw-rw-    1 1        1            5427 Jan  1 00:20 basic.cfg
-rwxrwxrwx    1 1        1           94145 Jan  1 00:20 basic.mdb
-rwxrwxrwx    1 1        1             677 Jan  1 01:17 key2.pub
drwxrwxrwx    1 1        1            2048 Jan  1 00:12 logfile
drwxrwxrwx    1 1        1            2048 Jan  1 01:32 new2
```

Exit SFTP client view.

```
sftp> quit

<SwitchA>
```

Configuration files

- Switch A:

```
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.105 255.255.255.0
#
 public-key peer 192.168.0.51
 public-key-code begin
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
```

```
    35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
    91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
    585DA7F42519718CC9B09EEF0381850002818100CE4A8B1F8AF6F5CE3D4D17F63E49A6780D
    A699ABD0601EC137B7E06FB710281055718FA3BB72118E1BD0CCBD366D8A214FF64A483A56
    388EA4EB2EC4CC34C166D081E61BD2A4D46BDD961931C0E1B58523372F17D2D634768BFF4E
    29C38C4960AE5957ACFDA2A6A1DE6970F093EE32A71C829B9BA701ECCD9715B066F814E788
  public-key-code end
  peer-public-key end
#
```

- Switch B:

```
#
 ftp server enable
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.51 255.255.255.0
#
 sftp server enable
 ssh user client002 service-type sftp authentication-type publickey assign publi
ckey Switch001
#
local-user client002 class manage
 service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
local-user ftp class manage
 password hash $h$6$CyLz0rqT0vizryPz$iCBbicrXu3ug+r2F18x2zpxDVSJkvMyiiDpj/h802VB
TyRFeJfsjOmY5seHI+tkYLtymUazqsNrGkaXVTLcL3Q==
 service-type ftp
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
 public-key peer Switch001
  public-key-code begin
    308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
    96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
    DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
    DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
    7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
    4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
    35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
    91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
    585DA7F42519718CC9B09EEF038184000281806D02F0D9F71F4B82356D6E4B6E91510609FE
    5E6F060F3ADCA2D92D375762E378945B68C741A07624A7EE09EA882985C43C8B84C7610F44
```

```
    B9EFB3140AF8E2E824D0865AD6AD00754AE9583F094BDDC509CAE1C521C941D6999F97AEA3
    5709A53D4BD497CBB8A412D3145609AB8D059037132006CF6D6A11F7B0965A35DEDA4DC6
  public-key-code end
 peer-public-key end
#
```

Example: Configuring SCP file transfer with password authentication

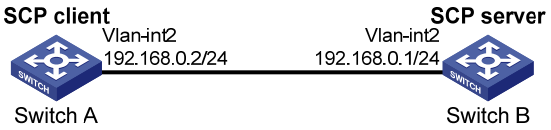
Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 226, you can log in to Switch B through the SCP client that runs on Switch A. After login, you are assigned the user role **network-admin** for simple file transferring operations. Switch B uses the password authentication. The username and password of the client are saved on Switch B.

Figure 226 Network diagram



Configuration restrictions and guidelines

When you configure the switch as an SCP client for password authentication, follow these restrictions and guidelines:

- When you try to access an SCP server, the client must use the server's host public key to authenticate the server. If you have not configured the server's host public key on the client, the client will ask you whether you want to continue with the access.
  - If you choose to continue, the client accesses the server and downloads the server's host public key.
  - If you choose to not continue, the connection cannot be established.

  In an insecure network, HP recommends that you configure the server's host public key on the client.
- The user role for the password authenticated SCP user is obtained by using one of the following methods:
  - Authorized by the remote AAA server.

    - Specified by the **authorization-attribute** command in the associated local user view.
- The working directory for the password authenticated SCP user is authorized by the AAA server.

Configuration procedures

Assign an IP address to VLAN-interface 2 on the SCP client. The SCP client uses this IP address to establish the SCP connection.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

Generate RSA key pairs.

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

Generate a DSA key pair.

```
[SwitchB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:2048
Generating Keys...
...........+...+.......+............+..+.......................+..+..+.....+..
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
......+.+.+.....+.................+......+................++++++++++++++++++++
++++++++++++++++++++++++++*
Create the key pair successfully.
```

Enable the SSH server function.

```
[SwitchB] ssh server enable
```

Create a local device management user named **client001** with the plaintext password **aabbcc**, the service type **ssh**, the user role **network-admin**, and the working directory **flash:/**.

```
[SwitchB] local-user client001 class manage
[SwitchB-luser-manage-client001] password simple aabbcc
[SwitchB-luser-manage-client001] service-type ssh
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] authorization-attribute work-directory flash:/
[SwitchB-luser-manage-client001] quit
```

Create an SSH user **client001** with the service type **scp** and the authentication method **password**. By default, password authentication is used if an SSH user is not created.

```
[SwitchB] ssh user client001 service-type scp authentication-type password
```

Verifying the configuration

Connect to the SCP server, download the file **basic.cfg** from the server, and save it locally with the name **local.cfg**.

```
<SwitchA> scp 192.168.0.1 get basic.cfg local.cfg
Username: client001
Connected to 192.168.0.1 ...
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
basic.cfg                                     100% 5427     5.3KB/s   00:00
```

Configuration files

The section displays the configuration files on Switch B.

```
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.1 255.255.255.0
#
 ssh server enable
 ssh user client001 service-type stelnet authentication-type password
#
local-user client001 class manage
 password hash $h$6$JM2d+CjyWo60Lx+z$QN5/eszOsB2t9nULUaEJVrEU4cZl3HNdYx1Gykx2bVk
IqEaxZD8Kh62gN/HHesf8Dnd/1USVMU6MTck2agnk6A==
 service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
```

Static multicast route configuration examples

This chapter provides static multicast route configuration examples.

General configuration restrictions and guidelines

When you configure a static multicast route, specify the RPF neighbor only by the neighbor's IP address rather than the type and number of the interface that is connected to the neighbor.

Example: Configuring static multicast routes (for changing RPF routes)

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

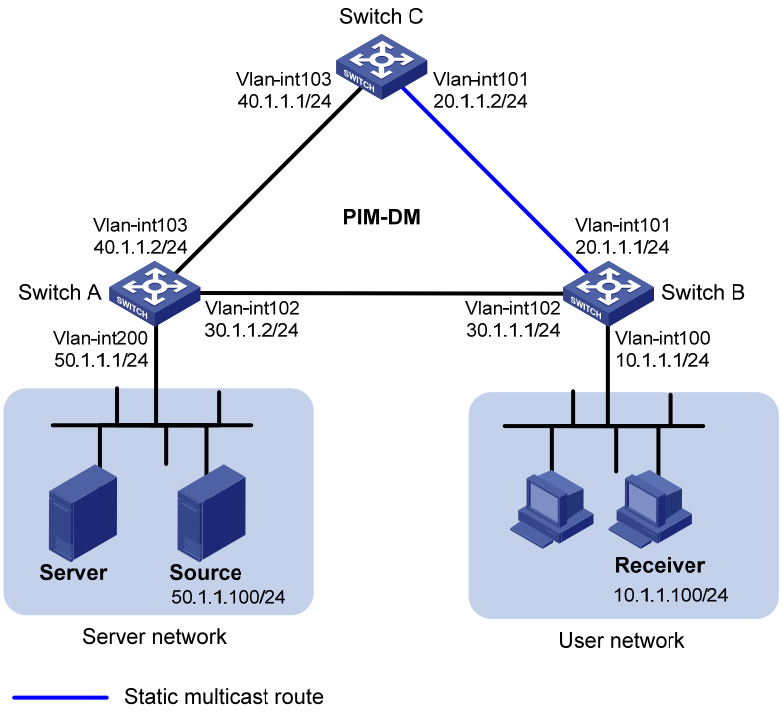
Network requirements

As shown in Figure 227:

- The server network and user network access the PIM-DM network through Switch A and Switch B, respectively.
- The server network sends a large amount of unicast packets and multicast packets to the user network.

To lessen the burden on unicast transmission path, configure a static multicast route on switch B so multicast packets travel along a different path than the path for unicast packets.

Figure 227 Network diagram



Requirement analysis

Before you configure a static multicast route, display the RPF neighbor information on Switch B and 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 the RPF neighbor of the unicast route.

Configuration procedures

1. Configure the IP address and subnet mask for each interface as shown in Figure 227. (Details not shown.)
2. Enable OSPF on the switches in the PIM-DM domain to make sure the following requirements are met: (Details not shown.)
   - The network layer on the PIM-DM network is interoperable.
   - The routing information among the switches can be dynamically updated.
3. Enable IP multicast routing, PIM-DM, and IGMP:

   # 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 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
```

On Switch C, enable IP multicast routing and PIM-DM 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
```

On Switch B, enable IGMP and PIM-DM on VLAN-interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim dm
[SwitchB-Vlan-interface100] quit
```

On Switch B, enable PIM-DM on VAN-interface 101 and VLAN-interface 102.

```
[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
```

4. Display the RPF route to Source on Switch B.

```
[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 that the current RPF route on Switch B is contributed by a unicast routing protocol and the RPF neighbor is Switch A.

5. Configure a static multicast route, specifying Switch C as its RPF neighbor on the route to Source.

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

Verifying the configuration

Display information about the RPF route to 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 Source on Switch B is the configured static multicast route.
- The RPF neighbor of Switch B is Switch C.

Configuration files

- 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.
 pim dm
 igmp enable
#
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 5900	Release 2208P01
HP 5920	Release 2210

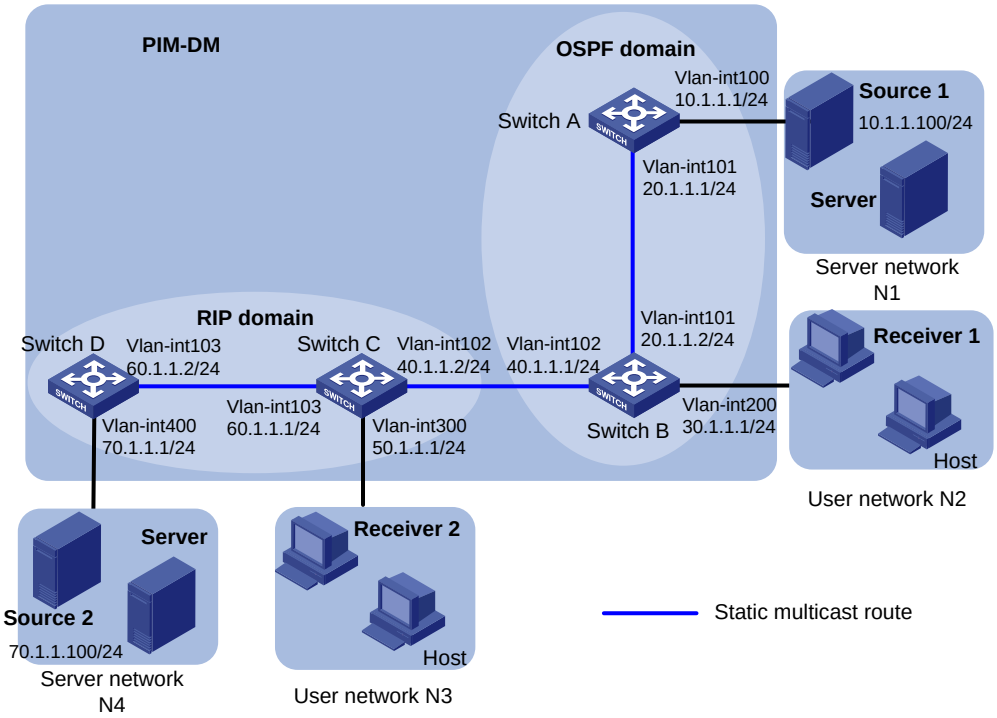
Network requirements

As shown in Figure 228:

- 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 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 228 Network diagram



Requirement analysis

To meet the network requirements, you must configure static multicast routes on the devices that are located between the receivers and the multicast source, and 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 228. (Details not shown.)
2. Enable OSPF on Switch A and Switch B to make sure the following requirements are met: (Details not shown.)
   - Switch A and Switch B are interoperable on the network layer.
   - The routing information among Switch A and Switch B can be dynamically updated.

3. Enable RIP on Switch C and Switch D to make sure the following requirements are met: (Details not shown.)
   - Switch C and Switch D are interoperable on the network layer.
   - The routing information among Switch C and Switch D can be dynamically updated.
4. Enable IP multicast routing, IGMP, and PIM-DM:

   # On Switch A, enable IP multicast routing globally, and enable PIM-DM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[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
```

   # On Switch B, enable IGMP and PIM-DM on VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit
```

   # On Switch B, enable PIM-DM on VLAN-interface 101 and VLAN-interface 102.

```
[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 routes to the multicast sources on Switch B and Switch C.

   # 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. No RPF routes to Source 2 exist on Switch B.

   # Display information about the RPF route to Source 1 on Switch C.

```
[SwitchC] display multicast rpf-info 10.1.1.100
```

   No output is displayed. 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 Source 1.

```
[SwitchC] ip rpf-route-static 10.1.1.100 24 40.1.1.1
```

Verifying the configuration

Display information about the RPF route to Source 2 on Switch B.

```
[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
```

Display information about the RPF route to Source 1 on Switch C.

```
[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 that the RPF routes to Source 2 and Source 1 are available on Switch B and Switch C, respectively, and they 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
 pim dm
 igmp enable
#
```

```
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 5900	Release 2208P01
HP 5920	Release 2210

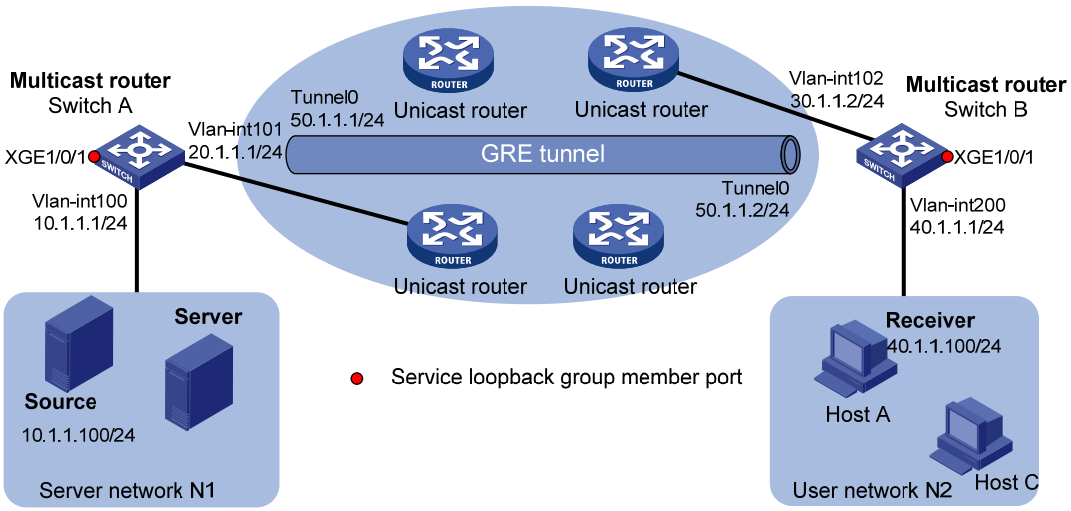
Network requirements

As shown in Figure 229:

- 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 a GRE over IPv4 tunnel between Switch A and Switch B, so Host A in N2 can receive multicast packets from the source in N1.

Figure 229 Network diagram



Requirements analysis

Configure a static multicast route to the multicast source at the receiver end of the tunnel. Specify 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 a 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.
- When you configure a GRE tunnel, create a service loopback group, specify its service type as **Tunnel**, and add an unused Layer 2 Ethernet port to the service loopback group.

Configuration procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 229. (Details not shown.)
2. Enable OSPF on switches to make sure the following requirements are met: (Details not shown.)
   - The network layer among the switches is interoperable.
   - The routing information among the switches can be dynamically updated.
3. Configure a GRE over IPv4 tunnel:

   # On Switch A, create interface Tunnel 0 and specify the tunnel encapsulation mode as GRE over IPv4.

   ```
   <SwitchA> system-view
   ```

```
[SwitchA] interface tunnel 0 mode gre
```

Assign an IP address and subnet mask to interface Tunnel 0, and specify its source and destination addresses.

```
[SwitchA-Tunnel0] ip address 50.1.1.1 24
[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
```

Add Ten-GigabitEthernet 1/0/1 to service loopback group 1. (Ten-GigabitEthernet 1/0/1 is an unused interface and does not belong to VLAN 100 or VLAN 101.)

```
[SwitchA] service-loopback group 1 type tunnel
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

On Switch B, create interface Tunnel 0, and specify the tunnel encapsulation mode as GRE over IPv4.

```
<SwitchB> system-view
[SwitchB] interface tunnel 0 mode gre
```

Assign an IP address and subnet mask to interface Tunnel 0, and specify its source and destination addresses.

```
[SwitchB-Tunnel0] ip address 50.1.1.2 24
[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
```

Add Ten-GigabitEthernet 1/0/1 to service loopback group 1. (Ten-GigabitEthernet 1/0/1 is an unused interface and does not belong to VLAN 102 or VLAN 200.)

```
[SwitchB] service-loopback group 1 type tunnel
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

4. 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
```

5. 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
```

6. On Switch B, configure a static multicast route, specifying interface Tunnel 0 on Switch A as the RPF neighbor toward the source.

```
[SwitchB] ip rpf-route-static 10.1.1.0 24 50.1.1.1
```

Verifying the configuration

Send an IGMP report from Host A to join the multicast group **225.1.1.1**. (Details not shown.)

Send multicast data from the multicast source to the multicast group **225.1.1.1**. (Details not shown.)

Display PIM routing table information on Switch B.

```
[SwitchB] display pim routing-table
 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: Vlan200
             Protocol: igmp, UpTime: 00:04:25, Expires: -
```

```
 (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: Vlan200
             Protocol: pim-dm, UpTime: 00:04:25, Expires: -
```

The output shows that Switch A is the RPF neighbor of Switch B and the multicast data from Switch A is delivered over a GRE tunnel to Switch B.

Configuration files

- Switch A:

```
#
service-loopback group 1 type tunnel
#
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
#
interface Ten-GigabitEthernet1/0/1
 port service-loopback group 1
#
interface Tunnel0 mode gre
 ip address 50.1.1.1 255.255.255.0
 pim dm
 source 20.1.1.1
 destination 30.1.1.2
#
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:

```
#
service-loopback group 1 type tunnel
#
```

```
multicast routing-enable
#

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
 pim dm
 igmp enable
#
interface Ten-GigabitEthernet1/0/1
 port service-loopback group 1
#
interface Tunnel0 mode gre
 ip address 50.1.1.2 255.255.255.0
 pim dm
 source 30.1.1.2
 destination 20.1.1.1
#
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
#
ip rpf-route-static 10.1.1.0 24 50.1.1.1
#
```

Task scheduling configuration examples

This document provides examples for scheduling tasks to make the device automatically execute a command or a set of commands without administrative interference.

Example: Scheduling tasks

Applicable product matrix

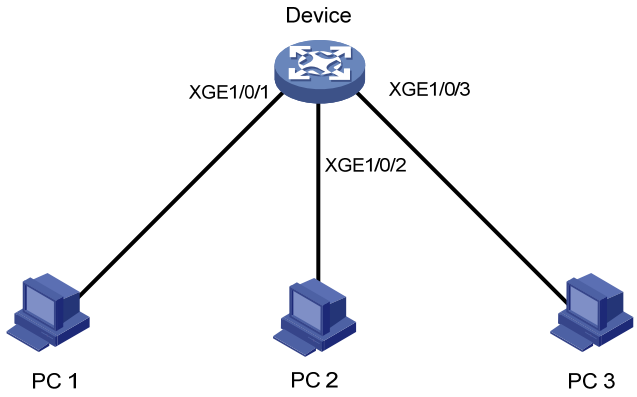
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

To save energy, configure the device to do the following:

- Enable interfaces Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 at 8:00 a.m. every Monday through Friday.
- Disable the interfaces at 18:00 every Monday through Friday.

Figure 230 Network diagram



Scheduling procedures

Enter system view.

```
<Sysname> system-view
```

Configure a job for disabling interface Ten-GigabitEthernet 1/0/1.

```
[Sysname] scheduler job shutdown-ten-gigabitethernet1/0/1
[Sysname-job-shutdown-ten-gigabitethernet1/0/1] command 1 system-view
[Sysname-job-shutdown-ten-gigabitethernet1/0/1] command 2 interface ten-gigabitethernet
1/0/1
```

```
[Sysname-job-shutdown-ten-gigabitethernet1/0/1] command 3 shutdown
[Sysname-job-shutdown-ten-gigabitethernet1/0/1] quit
```

Configure a job for enabling interface Ten-GigabitEthernet 1/0/1.

```
[Sysname] scheduler job start-ten-gigabitethernet1/0/1
[Sysname-job-start-ten-gigabitethernet1/0/1] command 1 system-view
[Sysname-job-start-ten-gigabitethernet1/0/1] command 2 interface ten-gigabitethernet
1/0/1
[Sysname-job-start-ten-gigabitethernet1/0/1] command 3 undo shutdown
[Sysname-job-start-ten-gigabitethernet1/0/1] quit
```

Configure a job for disabling interface Ten-GigabitEthernet 1/0/2.

```
[Sysname] scheduler job shutdown-ten-gigabitethernet1/0/2
[Sysname-job-shutdown-ten-gigabitethernet1/0/2] command 1 system-view
[Sysname-job-shutdown-ten-gigabitethernet1/0/2] command 2 interface ten-gigabitethernet
1/0/2
[Sysname-job-shutdown-ten-gigabitethernet1/0/2] command 3 shutdown
[Sysname-job-shutdown-ten-gigabitethernet1/0/2] quit
```

Configure a job for enabling interface Ten-GigabitEthernet 1/0/2.

```
[Sysname] scheduler job start-ten-gigabitethernet1/0/2
[Sysname-job-start-ten-gigabitethernet1/0/2] command 1 system-view
[Sysname-job-start-ten-gigabitethernet1/0/2] command 2 interface ten-gigabitethernet
1/0/2
[Sysname-job-start-ten-gigabitethernet1/0/2] command 3 undo shutdown
[Sysname-job-start-ten-gigabitethernet1/0/2] quit
```

Configure a periodic schedule for enabling the interfaces at 8:00 a.m. every Monday through Friday.

```
[Sysname] scheduler schedule START-PC1/PC2
[Sysname-schedule-START-PC1/PC2] job start-ten-gigabitethernet1/0/1
[Sysname-schedule-START-PC1/PC2] job start-ten-gigabitethernet1/0/2
[Sysname-schedule-START-PC1/PC2] time repeating at 8:00 week-day mon tue wed thu fri
[Sysname-schedule-START-PC1/PC2] quit
```

Configure a periodic schedule for disabling the interfaces at 18:00 every Monday through Friday.

```
[Sysname] scheduler schedule STOP-PC1/PC2
[Sysname-schedule-STOP-PC1/PC2] job shutdown-ten-gigabitethernet1/0/1
[Sysname-schedule-STOP-PC1/PC2] job shutdown-ten-gigabitethernet1/0/2
[Sysname-schedule-STOP-PC1/PC2] time repeating at 18:00 week-day mon tue wed thu fri
[Sysname-schedule-STOP-PC1/PC2] quit
```

Verifying the scheduling

Display the configuration information of all jobs.

```
[Sysname] display scheduler job
Job name: shutdown-ten-gigabitethernet1/0/1
 system-view
 interface ten-gigabitethernet1/0/1
 shutdown

Job name: shutdown-ten-gigabitethernet1/0/2
 system-view
```

```
 interface ten-gigabitethernet1/0/2
 shutdown

Job name: start-ten-gigabitethernet1/0/1
 system-view
 interface ten-gigabitethernet1/0/1
 undo shutdown

Job name: start-ten-gigabitethernet1/0/2
 system-view
 interface ten-gigabitethernet1/0/2
 undo shutdown
```

Display the schedule information.

```
[Sysname] display scheduler schedule
Schedule name        : START-PC1/PC2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time           : Wed Sep 25 08:00:00 2013
Last execution time  : Wed Sep 25 08:00:00 2013
Last completion time : Wed Sep 25 08:00:03 2013
Execution counts     : 1
------------------------------------------------------------------------
Job name                                        Last execution status
start-ten-gigabitethernet1/0/1                  Successful
start-ten-gigabitethernet1/0/2                  Successful

Schedule name        : STOP-PC1/PC2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time           : Wed Sep 25 18:00:00 2013
Last execution time  : Wed Sep 25 18:00:00 2013
Last completion time : Wed Sep 25 18:00:01 2013
Execution counts     : 1
------------------------------------------------------------------------
Job name                                        Last execution status
shutdown-ten-gigabitethernet1/0/1               Successful
shutdown-ten-gigabitethernet1/0/2               Successful
```

Display schedule log information.

```
[Sysname] display scheduler logfile
Logfile Size: 1440 Bytes.

Job name        : start-ten-gigabitethernet1/0/1
Schedule name   : START-PC1/PC2
Execution time  : Wed Sep 25 08:00:00 2013
Completion time : Wed Sep 25 08:00:02 2013
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1]undo shutdown
```

```
Job name        : start-ten-gigabitethernet1/0/2
Schedule name   : START-PC1/PC2
Execution time  : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
---------------------------------- Job output ----------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitethernet 1/0/2
[Sysname-Ten-GigabitEthernet1/0/2]undo shutdown

Job name        : shutdown-ten-gigabitethernet1/0/1
Schedule name   : STOP-PC1/PC2
Execution time  : Wed Sep 25 18:00:00 2013
Completion time : Wed Sep 25 18:00:01 2013
---------------------------------- Job output ----------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1]shutdown

Job name        : shutdown-ten-gigabitethernet1/0/2
Schedule name   : STOP-PC1/PC2
Execution time  : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
---------------------------------- Job output ----------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitethernet 1/0/2
[Sysname-Ten-GigabitEthernet1/0/2]shutdown
```

Configuration files

```
#
scheduler job shutdown-ten-gigabitethernet1/0/1
 command 1 system-view
 command 2 interface ten-gigabitethernet 1/0/1
 command 3 shutdown
#
scheduler job shutdown-ten-gigabitethernet1/0/2
 command 1 system-view
 command 2 interface ten-gigabitethernet 1/0/2
 command 3 shutdown
#
scheduler job start-ten-gigabitethernet1/0/1
 command 1 system-view
 command 2 interface ten-gigabitethernet 1/0/1
 command 3 undo shutdown
```

```
#
scheduler job start-ten-gigabitethernet1/0/2
 command 1 system-view
 command 2 inter ten-gigabitethernet 1/0/2
 command 3 undo shutdown
#
scheduler schedule START-PC1/PC2
 job start-ten-gigabitethernet1/0/1
 job start-ten-gigabitethernet1/0/2
 time repeating at 08:00 week-day Mon Tue Wed Thu Fri
#
scheduler schedule STOP-PC1/PC2
 job shutdown-ten-gigabitethernet1/0/1
 job shutdown-ten-gigabitethernet1/0/2
 time repeating at 18:00 week-day Mon Tue Wed Thu Fri
#
```

TRILL configuration examples

This chapter provides configuration examples for using TRILL together with IRF.

Example: Configuring TRILL

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

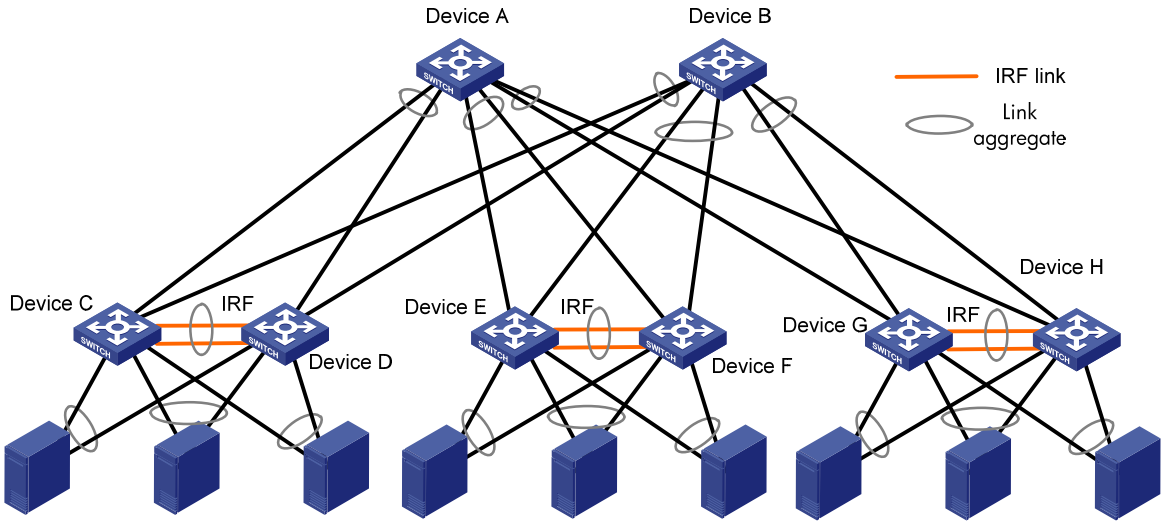
As shown in Figure 231:

- Device C, Device D, Device E, Device F, Device G, and Device H are the access layer devices of the data center. The following pairs of devices form IRF fabrics:
  - Device C and Device D.
  - Device E and Device F.
  - Device G and Device H.
- The servers are connected to IRF fabrics at the access layer through aggregate links.
- The IRF fabrics at the access layer are connected to Device A and Device B at the distribution layer through aggregate links.

Configure TRILL to meet the following requirements:

- Avoid loops and implement multi-path forwarding for Layer 2 traffic between servers.
- Configure Device A and Device B as the distribution tree roots.

Figure 231 Network diagram



Configuration restrictions and guidelines

Because devices in this example have dense ports, the ports are numbered as follows on devices in Figure 231:

- On Device A and Device B, the ports are numbered as XGE 1/0/1 through XGE 1/0/6 from the left to the right, counter-clockwise.
- On Device C, Device E, and Device G:
  - The physical IRF ports are numbered as XGE 1/0/45 through XGE 1/0/48.
  - The other ports are numbered as XGE 1/0/1 through XGE 1/0/5 clockwise, starting from the port connecting to Device A.
- On Device D, Device F, and Device H:
  - The physical IRF ports are numbered as XGE 2/0/45 through XGE 2/0/48.
  - The other ports are numbered as XGE 2/0/1 through XGE 2/0/5 clockwise, starting from the port connecting to Device A.
- The servers are Server 1 through Server 9 from the left to the right.

Configuration procedures

Using Device C and Device D to form an IRF fabric (IRF_1)

1. Configure Device C:

   # Select SFP+ ports Ten-GigabitEthernet 1/0/45 through Ten-GigabitEthernet 1/0/48 as the physical IRF ports. Shut down these ports.

   ```
   <DeviceC> system-view
   [DeviceC] interface range ten-gigabitethernet 1/0/45 to ten-gigabitethernet 1/0/48
   [DeviceC-if-range] shutdown
   [DeviceC-if-range] quit
   ```

NOTE:

To facilitate the configuration, you can use an interface range to bulk shut down and bring up these ports.

Bind IRF-port 1/1 to physical ports Ten-GigabitEthernet 1/0/45 through Ten-GigabitEthernet 1/0/48.

```
[DeviceC] irf-port 1/1
[DeviceC-irf-port1/1] port group interface ten-gigabitethernet 1/0/45
[DeviceC-irf-port1/1] port group interface ten-gigabitethernet 1/0/46
[DeviceC-irf-port1/1] port group interface ten-gigabitethernet 1/0/47
[DeviceC-irf-port1/1] port group interface ten-gigabitethernet 1/0/48
[DeviceC-irf-port1/1] quit
```

Bring up GigabitEthernet 1/0/45 through GigabitEthernet 1/0/48, and save the configuration.

```
[DeviceC] interface range ten-gigabitethernet 1/0/45 to ten-gigabitethernet 1/0/48
[DeviceC-if-range] undo shutdown
[DeviceC-if-range] quit
[DeviceC] save
```

Activate the IRF port.

```
[DeviceC] irf-port-configuration active
```

2. Configure Device D:

Change the IRF member ID of Device D from 1 to 2. Reboot Device D to make the new ID take effect.

```
<DeviceD> system-view
[DeviceD] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[DeviceD] quit
<DeviceD> reboot
```

Select SFP+ ports Ten-GigabitEthernet 2/0/45 through Ten-GigabitEthernet 2/0/48 as the physical IRF ports. Connect these ports to ports Ten-GigabitEthernet 1/0/45 through Ten-GigabitEthernet 1/0/48 of Device C, respectively.

Log in to Device D, and bulk shut down ports Ten-GigabitEthernet 2/0/45 through Ten-GigabitEthernet 2/0/48.

```
<DeviceD> system-view
[DeviceD] interface range ten-gigabitethernet 2/0/45 to ten-gigabitethernet 2/0/48
[DeviceD-if-range] shutdown
[DeviceD-if-range] quit
```

Bind IRF-port 2/2 to physical ports Ten-GigabitEthernet 2/0/45 through Ten-GigabitEthernet 2/0/48.

```
[DeviceD] irf-port 2/2
[DeviceD-irf-port2/2] port group interface ten-gigabitethernet 2/0/45
[DeviceD-irf-port2/2] port group interface ten-gigabitethernet 2/0/46
[DeviceD-irf-port2/2] port group interface ten-gigabitethernet 2/0/47
[DeviceD-irf-port2/2] port group interface ten-gigabitethernet 2/0/48
[DeviceD-irf-port2/2] quit
```

Bring up GigabitEthernet 2/0/45 through GigabitEthernet 2/0/48, and save the configuration.

```
[DeviceD] interface range ten-gigabitethernet 2/0/45 to ten-gigabitethernet 2/0/48
[DeviceD-if-range] undo shutdown
[DeviceD-if-range] quit
[DeviceD] save
```

Activate the IRF port.

```
[DeviceD] irf-port-configuration active
```

After you configure Device C and Device D, they participate in the master device election. The device that fails the election reboots. After the reboot, IRF fabric IRF_1 is formed.

Using Device E and Device F to form an IRF fabric (IRF_2)

Use Device E and Device F to form IRF_2 in the same way IRF_1 is formed.

Using Device G and Device H to form an IRF fabric (IRF_3)

Use Device G and Device H to form IRF_3 in the same way IRF_1 is formed.

Configuring aggregate interfaces on IRF_1, IRF_2, and IRF_3 for connecting to Device A and Device B

1. Configure IRF_1:

   # Create dynamic Layer 2 aggregate interface 1 for connecting to Device A.

   ```
   <IRF_1> system-view
   [IRF_1] interface bridge-aggregation 1
   [IRF_1-Bridge-Aggregation1] link-aggregation mode dynamic
   [IRF_1-Bridge-Aggregation1] quit
   ```

   # Assign ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 2/0/1 to Layer 2 aggregation group 1.

   ```
   [IRF_1] interface ten-gigabitethernet 1/0/1
   [IRF_1-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   [IRF_1-Ten-GigabitEthernet1/0/1] quit
   [IRF_1] interface ten-gigabitethernet 2/0/1
   [IRF_1-Ten-GigabitEthernet2/0/1] port link-aggregation group 1
   [IRF_1-Ten-GigabitEthernet2/0/1] quit
   ```

   # Create dynamic Layer 2 aggregate interface 2 for connecting to Device B.

   ```
   [IRF_1] interface bridge-aggregation 2
   [IRF_1-Bridge-Aggregation2] link-aggregation mode dynamic
   [IRF_1-Bridge-Aggregation2] quit
   ```

   # Assign ports Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 2/0/2 to aggregation group 2.

   ```
   [IRF_1] interface ten-gigabitethernet 1/0/2
   [IRF_1-Ten-GigabitEthernet1/0/2] port link-aggregation group 2
   [IRF_1-Ten-GigabitEthernet1/0/2] quit
   [IRF_1] interface ten-gigabitethernet 2/0/2
   [IRF_1-Ten-GigabitEthernet2/0/2] port link-aggregation group 2
   [IRF_1-Ten-GigabitEthernet2/0/2] quit
   ```

2. Configure IRF_2 and IRF_3 in the same way IRF_1 is configured.

Configuring aggregate interfaces on IRF_1, IRF_2, and IRF_3 for connecting to servers

IMPORTANT:

- The servers in this example must support link aggregation.
- When dynamic aggregate interfaces on IRF_1, IRF_2, and IRF_3 cannot connect to servers, try using static aggregate interfaces.

HP recommends using static link aggregation. This section uses static aggregate interfaces.

1. Configure IRF_1:

   # Create static Layer 2 aggregate interface 3 for connecting to Server 3.

```
<IRF_1> system-view
[IRF_1] interface bridge-aggregation 3
[IRF_1-Bridge-Aggregation3] quit
```

   # Assign ports Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 2/0/3 to aggregation group 3.

```
[IRF_1] interface ten-gigabitethernet 1/0/3
[IRF_1-Ten-GigabitEthernet1/0/3] port link-aggregation group 3
[IRF_1-Ten-GigabitEthernet1/0/3] quit
[IRF_1] interface ten-gigabitethernet 2/0/3
[IRF_1-Ten-GigabitEthernet2/0/3] port link-aggregation group 3
[IRF_1-Ten-GigabitEthernet2/0/3] quit
```

   # Create static Layer 2 aggregate interface 4 for connecting to Server 2.

```
[IRF_1] interface bridge-aggregation 4
[IRF_1-Bridge-Aggregation4] quit
```

   # Assign ports Ten-GigabitEthernet 1/0/4 and Ten-GigabitEthernet 2/0/4 to aggregation group 4.

```
[IRF_1] interface ten-gigabitethernet 1/0/4
[IRF_1-Ten-GigabitEthernet1/0/4] port link-aggregation group 4
[IRF_1-Ten-GigabitEthernet1/0/4] quit
[IRF_1] interface ten-gigabitethernet 2/0/4
[IRF_1-Ten-GigabitEthernet2/0/4] port link-aggregation group 4
[IRF_1-Ten-GigabitEthernet2/0/4] quit
```

   # Create static Layer 2 aggregate interface 5 for connecting to Server 1.

```
[IRF_1] interface bridge-aggregation 5
[IRF_1-Bridge-Aggregation5] quit
```

   # Assign ports Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 2/0/5 to aggregation group 5.

```
[IRF_1] interface ten-gigabitethernet 1/0/5
[IRF_1-Ten-GigabitEthernet1/0/5] port link-aggregation group 5
[IRF_1-Ten-GigabitEthernet1/0/5] quit
[IRF_1] interface ten-gigabitethernet 2/0/5
[IRF_1-Ten-GigabitEthernet2/0/5] port link-aggregation group 5
[IRF_1-Ten-GigabitEthernet2/0/5] quit
```

2. Configure IRF_2 and IRF_3 in the same way IRF_1 is configured.

Configuring aggregate interfaces on Device A and Device B for connecting to access layer devices

1. Configure Device A:

   # Create dynamic Layer 2 aggregate interface 1 for connecting to IRF_1.

```
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 1.

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

Create dynamic Layer 2 aggregate interface 2 for connecting to IRF_2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] quit
```

Assign ports Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 2.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 2
[DeviceA-Ten-GigabitEthernet1/0/3] quit
[DeviceA] interface ten-gigabitethernet 1/0/4
[DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 2
[DeviceA-Ten-GigabitEthernet1/0/4] quit
```

Create dynamic Layer 2 aggregate interface 3 for connecting to IRF_3.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] quit
```

Assign ports Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 to aggregation group 3.

```
[DeviceA] interface ten-gigabitethernet 1/0/5
[DeviceA-Ten-GigabitEthernet1/0/5] port link-aggregation group 3
[DeviceA-Ten-GigabitEthernet1/0/5] quit
[DeviceA] interface ten-gigabitethernet 1/0/6
[DeviceA-Ten-GigabitEthernet1/0/6] port link-aggregation group 3
[DeviceA-Ten-GigabitEthernet1/0/6] quit
```

2. Configure Device B in the same way Device A is configured.

Configuring TRILL

1. Configure the downlink ports for access layer devices IRF_1, IRF_2, and IRF_3:

Enable TRILL globally on IRF_1. Enable TRILL on static aggregate interfaces 3, 4, and 5.

```
<IRF_1> system-view
[IRF_1] trill
[IRF_1-trill] quit
[IRF_1] interface Bridge-Aggregation 3
[IRF_1-Bridge-Aggregation3] trill enable
[IRF_1-Bridge-Aggregation3] quit
```

```
[IRF_1] interface Bridge-Aggregation 4
[IRF_1-Bridge-Aggregation4] trill enable
[IRF_1-Bridge-Aggregation4] quit
[IRF_1] interface Bridge-Aggregation 5
[IRF_1-Bridge-Aggregation5] trill enable
[IRF_1-Bridge-Aggregation5] quit
```

Configure IRF_2 and IRF_3 in the same way IRF_1 is configured.

2. Configure the uplink ports for access layer devices IRF_1, IRF_2, and IRF_3:
   - Enable TRILL on uplink ports and dynamic aggregate interfaces 1 and 2.
   - Configure these ports as trunk ports.

```
[IRF_1] interface Bridge-Aggregation 1
[IRF_1-Bridge-Aggregation1] trill enable
[IRF_1-Bridge-Aggregation1] trill link-type trunk
[IRF_1-Bridge-Aggregation1] quit
[IRF_1] interface Bridge-Aggregation 2
[IRF_1-Bridge-Aggregation2] trill enable
[IRF_1-Bridge-Aggregation2] trill link-type trunk
[IRF_1-Bridge-Aggregation2] quit
```

Configure IRF_2 and IRF_3 in the same way IRF_1 is configured.

3. Configure the downlink ports of distribution layer devices Device A and Device B:
   - Enable TRILL globally on Device A.
   - Enable TRILL on downlink ports and dynamic aggregate interfaces 1, 2, and 3.
   - Configure these ports as trunk ports.

```
<DeviceA> system-view
[DeviceA] trill
[DeviceA-trill] quit
[DeviceA] interface Bridge-Aggregation 1
[DeviceA-Bridge-Aggregation1] trill enable
[DeviceA-Bridge-Aggregation1] trill link-type trunk
[DeviceA-Bridge-Aggregation1] quit
[DeviceA] interface Bridge-Aggregation 2
[DeviceA-Bridge-Aggregation2] trill enable
[DeviceA-Bridge-Aggregation2] trill link-type trunk
[DeviceA-Bridge-Aggregation2] quit
[DeviceA] interface Bridge-Aggregation 3
[DeviceA-Bridge-Aggregation3] trill enable
[DeviceA-Bridge-Aggregation3] trill link-type trunk
[DeviceA-Bridge-Aggregation3] quit
```

Configure Device B in the same way Device A is configured.

4. Configure the uplink ports of distribution layer devices Device A and Device B:

Enable TRILL on uplink ports. This example uses Ten-GigabitEthernet1/0/7.

```
[DeviceA] interface ten-gigabitethernet 1/0/7
[DeviceA-Ten-GigabitEthernet1/0/7] trill enable
[DeviceA-Ten-GigabitEthernet1/0/7] quit
```

Configure Device B in the same way Device A is configured.

5. Configure TRILL distribution trees:

   # Set Device A's priority for selecting the root bridge of the distribution tree to 65535. Set the number of distribution trees that Device A wants all RBs to compute to 2.

   ```
   [DeviceA] trill
   [DeviceA-trill] tree-root priority 65535
   [DeviceA-trill] trees calculate 2
   [DeviceA-trill] quit
   ```

   # Set Device B's priority for selecting the root bridge of the distribution tree to 65534. Set the number of distribution trees that Device B wants all RBs to compute to 2.

   ```
   [DeviceB] trill
   [DeviceB-trill] tree-root priority 65534
   [DeviceB-trill] trees calculate 2
   [DeviceB-trill] quit
   ```

Verifying the configuration

1. Verify that no loop occurs in the network.
2. Verify that servers connected to different access layer devices can communicate with each other.
3. Display the MAC address table of IRF_1.

   In the output:

   - The **Port/NickName** fields for Server 4, Server 5, and Server 6 are all the nickname of IRF_2.
   - The **Port/NickName** fields for Server 7, Server 8, and Server 9 are all the nickname of IRF_3.

   The outputs on IRF_2 and IRF_3 are similar to the output on IRF_1.

Configuration files

- Device A:

```
#
trill
 tree-root priority 65535
 trees calculate 2
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Bridge-Aggregation2
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
```

```
#
interface Ten-GigabitEthernet1/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/3
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/4
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/5
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/6
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/7
 trill enable
#
```

- Device B:

```
#
trill
 tree-root priority 65534
 trees calculate 2
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Bridge-Aggregation2
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Ten-GigabitEthernet1/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
 port link-aggregation group 1
```

```
#
interface Ten-GigabitEthernet1/0/3
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/4
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/5
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/6
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/7
 trill enable
#
```

- IRF_1, IRF_2, and IRF_3:

```
#
trill
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/45
 port group interface Ten-GigabitEthernet1/0/46
 port group interface Ten-GigabitEthernet1/0/47
 port group interface Ten-GigabitEthernet1/0/48
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/45
 port group interface Ten-GigabitEthernet2/0/46
 port group interface Ten-GigabitEthernet2/0/47
 port group interface Ten-GigabitEthernet2/0/48
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Bridge-Aggregation2
 link-aggregation mode dynamic
 trill enable
 trill link-type trunk
#
interface Bridge-Aggregation3
 trill enable
#
interface Bridge-Aggregation4
 trill enable
#
```

```
interface Bridge-Aggregation5
 trill enable
#
interface Ten-GigabitEthernet1/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/3
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/4
 port link-aggregation group 4
#
interface Ten-GigabitEthernet1/0/5
 port link-aggregation group 5
#
interface Ten-GigabitEthernet2/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet2/0/3
 port link-aggregation group 3
#
interface Ten-GigabitEthernet2/0/4
 port link-aggregation group 4
#
interface Ten-GigabitEthernet2/0/5
 port link-aggregation group 5
#
```

Tunneling configuration examples

This chapter provides examples for configuring tunneling to transfer one network protocol by using another network protocol.

General configuration restrictions and guidelines

Before you configure a tunnel interface, create a tunnel-type service loopback group and add an unused Layer 2 Ethernet interface into the group.

Example: Configuring an IPv6 over IPv4 manual tunnel

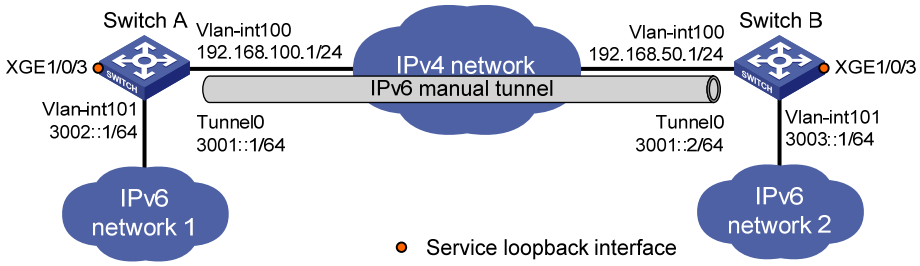
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 232, Switch A and Switch B can reach each other through IPv4. Configure an IPv6 over IPv4 manual tunnel between Switch A and Switch B so IPv6 network 1 and IPv6 network 2 can reach each other over the IPv4 network.

Figure 232 Network diagram



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 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 mode ipv6-ipv4
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] destination 192.168.50.1
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IPv6 network 2 through tunnel interface Tunnel 0.

```
[SwitchA] ipv6 route-static 3003:: 64 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 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 mode ipv6-ipv4
[SwitchB-Tunnel0] ipv6 address 3001::2/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] destination 192.168.100.1
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IPv6 network 1 through tunnel interface Tunnel 0.

```
[SwitchB] ipv6 route-static 3002:: 64 tunnel 0
```

Verifying the configuration

Ping the IPv6 address of VLAN-interface 101 on Switch B from Switch A. The ping operation succeeds.

```
[SwitchA] ping ipv6 3003::1
Ping6(56 data bytes) 3001::1 --> 3003::1, press CTRL_C to break
56 bytes from 3003::1, icmp_seq=0 hlim=64 time=45.000 ms
56 bytes from 3003::1, icmp_seq=1 hlim=64 time=10.000 ms
56 bytes from 3003::1, icmp_seq=2 hlim=64 time=4.000 ms
56 bytes from 3003::1, icmp_seq=3 hlim=64 time=10.000 ms
56 bytes from 3003::1, icmp_seq=4 hlim=64 time=11.000 ms

--- Ping6 statistics for 3003::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/16.000/45.000/14.711 ms
```

Configuration files

- Switch A:

```
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6-ipv4
 ipv6 address 3001::1/64
 source Vlan-interface100
 destination 192.168.50.1
#
 ipv6 route-static 3003:: 64 Tunnel0
#
```

- Switch B:

```
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6-ipv4
 ipv6 address 3001::2/64
 source Vlan-interface100
 destination 192.168.100.1
#
 ipv6 route-static 3002:: 64 Tunnel0
#
```

Example: Configuring a 6to4 tunnel

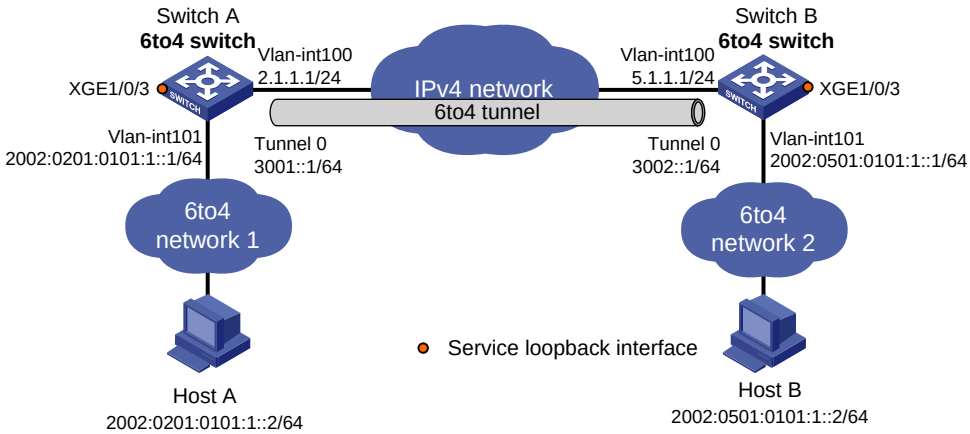
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 233, Switch A and Switch B can reach each other through IPv4. Configure a 6to4 tunnel between 6to4 switches Switch A and Switch B so Host A and Host B can reach each other over the IPv4 network.

Figure 233 Network diagram



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 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 mode ipv6-ipv4 6to4
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

Assign Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to 2002::/16 through tunnel interface Tunnel 0.

```
[SwitchA] ipv6 route-static 2002:: 16 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 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 mode ipv6-ipv4 6to4
[SwitchB-Tunnel0] ipv6 address 3002::1/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] quit
```

Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

Assign Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to 2002::/16 through tunnel interface Tunnel 0.

```
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0
```

Verifying the configuration

Ping Host B from Host A. The ping operation succeeds.

```
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:

```
#
 service-loopback group 1 type tunnel
#
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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6-ipv4 6to4
 ipv6 address 3001::1/64
 source Vlan-interface100
#
 ipv6 route-static 2002:: 16 Tunnel0
#
```

- Switch B:

```
#
 service-loopback group 1 type tunnel
#
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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6-ipv4 6to4
 ipv6 address 3002::1/64
 source Vlan-interface100
#
 ipv6 route-static 2002:: 16 Tunnel0
#
```

Example: Configuring an ISATAP tunnel

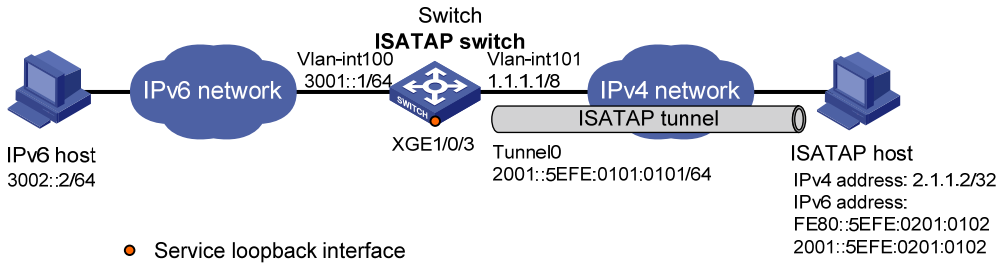
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 234, configure an ISATAP tunnel between the switch and the ISATAP host so the ISATAP host in the IPv4 network can access the IPv6 network.

Figure 234 Network diagram



Configuration procedures

Configuring the switch

Specify IP addresses for interfaces.

```
<Switch> system-view
[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 mode ipv6-ipv4 isatap
[Switch-Tunnel0] ipv6 address 2001::/64 eui-64
[Switch-Tunnel0] source vlan-interface 101
```

Disable RA suppression so that the ISATAP host can acquire information such as the address prefix from 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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[Switch] interface Ten-GigabitEthernet 1/0/3
[Switch-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[Switch-Ten-GigabitEthernet1/0/3] quit
```

Configuring the ISATAP host

Configurations on the ISATAP host vary with the operating systems. The following example is performed on Windows XP.

Install IPv6.

```
C:\>ipv6 install
```

On a host running Windows XP, the ISATAP interface is typically 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. The ping operation succeeds, indicating 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
```

Ping the IPv6 host from the ISATAP host. The ping operation succeeds.

```
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

```
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6-ipv4 isatap
 ipv6 address 2001::/64 eui-64
 undo ipv6 nd ra halt
 source Vlan-interface101
#
```

Example: Configuring an IPv4 over IPv4 tunnel

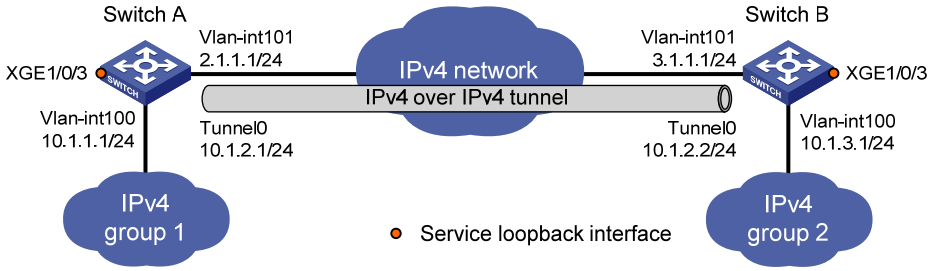
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 235, Switch A and Switch B can reach each other through IPv4. The two subnets group 1 and group 2 use private IPv4 addresses. Configure an IPv4 over IPv4 tunnel between Switch A and Switch B so the two subnets can reach each other.

Figure 235 Network diagram



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 mode ipv4-ipv4
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IP network group 2 through tunnel interface Tunnel 0.

```
[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 mode ipv4-ipv4
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IP network group 1 through tunnel interface Tunnel 0.

```
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

Verifying the configuration

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch A. The ping operation succeeds.

```
[SwitchA] ping -a 10.1.1.1 10.1.3.1
Ping 10.1.3.1 (10.1.3.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.3.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 10.1.3.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.3.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.3.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.3.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 10.1.3.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.000/1.000/2.000/0.632 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv4-ipv4
 ip address 10.1.2.1 255.255.255.0
 source 2.1.1.1
 destination 3.1.1.1
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv4-ipv4
 ip address 10.1.2.2 255.255.255.0
 source 3.1.1.1
 destination 2.1.1.1
#
 ip route-static 10.1.1.0 255.255.255.0 Tunnel0
#
```

Example: Configuring an IPv4 over IPv6 tunnel

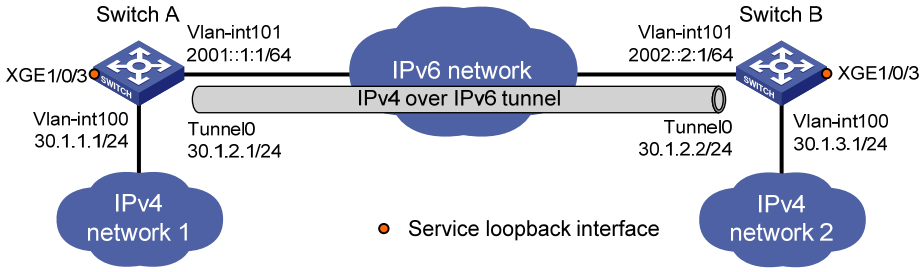
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 236, Switch A and Switch B can reach each other through IPv6. 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 236 Network diagram



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 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 mode ipv6
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel0] ip address 30.1.2.1 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IPv4 network 2 through tunnel interface Tunnel 0.

```
[SwitchA] ip route-static 30.1.3.0 255.255.255.0 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 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 mode ipv6
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel0] ip address 30.1.2.2 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IPv4 network 1 through tunnel interface Tunnel 0.

```
[SwitchB] ip route-static 30.1.1.0 255.255.255.0 tunnel 0
```

Verifying the configuration

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch A. The ping operation succeeds.

```
[SwitchA] ping -a 30.1.1.1 30.1.3.1
Ping 30.1.3.1 (30.1.3.1) from 30.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 30.1.3.1: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 30.1.3.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 30.1.3.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 30.1.3.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 30.1.3.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 30.1.3.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.000/1.200/3.000/0.980 ms
```

Configuration files

- Switch A:

```
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6
 ip address 30.1.2.1 255.255.255.0
 source 2001::1:1
 destination 2002::2:1
#
ip route-static 30.1.3.0 255.255.255.0 Tunnel0
#
```

- Switch B:

```
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
```

```
 ip address 30.1.3.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002::2:1/64
#
interface Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6
 ip address 30.1.2.2 255.255.255.0
 source 2002::2:1
 destination 2001::1:1
#
ip route-static 30.1.1.0 255.255.255.0 Tunnel0
#
```

Example: Configuring an IPv6 over IPv6 tunnel

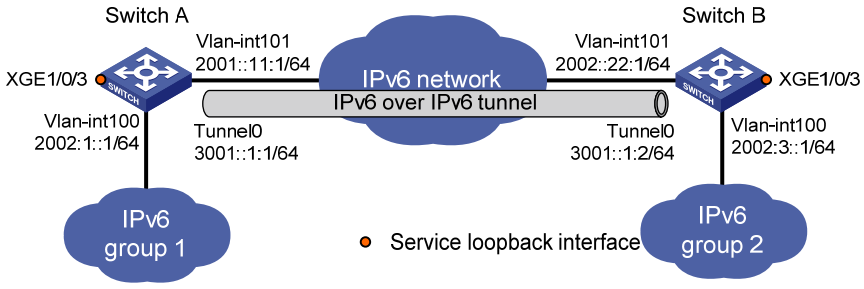
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 237, Switch A and Switch B can reach each other through IPv6. 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 237 Network diagram



Configuration procedures

Configuring Switch A

Specify an IPv6 address for VLAN-interface 100.

```
<SwitchA> system-view
[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 mode ipv6
```

Specify an IPv6 address for the tunnel interface.

```
[SwitchA-Tunnel0] ipv6 address 3001::1:1 64
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IPv6 network group 2 through tunnel interface Tunnel 0.

```
[SwitchA] ipv6 route-static 2002:3:: 64 tunnel 0
```

Configuring Switch B

Specify an IPv6 address for VLAN-interface 100.

```
<SwitchB> system-view
[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 mode ipv6
```

Specify an IPv6 address for the tunnel interface.

```
[SwitchB-Tunnel0] ipv6 address 3001::1:2 64
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IPv6 network group 1 through tunnel interface Tunnel 0.

```
[SwitchB] ipv6 route-static 2002:1:: 64 tunnel 0
```

Verifying the configuration

Ping the IPv6 address of the peer interface VLAN-interface 100 from Switch A. The ping operation succeeds.

```
[SwitchA] ping ipv6 -a 2002:1::1 2002:3::1
Ping6(56 data bytes) 2002:1::1 --> 2002:3::1, press CTRL_C to break
56 bytes from 2002:3::1, icmp_seq=0 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=3 hlim=64 time=0.000 ms
56 bytes from 2002:3::1, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for 2002:3::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms
```

Configuration files

- SwitchA:

```
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6
```

```
 ipv6 address 3001::1:1/64
 source 2001::11:1
 destination 2002::22:1
#
ipv6 route-static 2002:3:: 64 Tunnel0
#
```

- SwitchB:

```
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode ipv6
 ipv6 address 3001::1:2/64
 source 2002::2:1
 destination 2001::11:1
#
ipv6 route-static 2002:1:: 64 Tunnel0
#
```

Example: Configuring a GRE over IPv4 tunnel

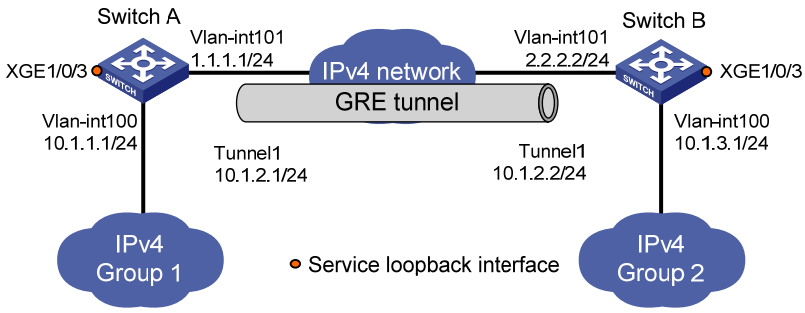
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 238, Switch A and Switch B can reach each other through IPv4. Configure a GRE 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 238 Network diagram



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 mode gre
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel1] ip address 10.1.2.1 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IP network Group 2 through tunnel interface Tunnel 1.

```
[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 mode gre
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel1] ip address 10.1.2.2 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IP network Group 1 through tunnel interface Tunnel 1.

```
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 Tunnel 1
```

Verifying the configuration

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch B. The ping operation succeeds.

```
[SwitchB] ping -a 10.1.3.1 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.1.3.1: 56 data bytes
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=11.000 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- 10.1.1.1 ping statistics ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.000/2.400/11.000/4.317 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel1 mode gre
 ip address 10.1.2.1 255.255.255.0
 source Vlan-interface101
 destination 2.2.2.2
#
 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 Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel1 mode gre
 ip address 10.1.2.2 255.255.255.0
 source Vlan-interface101
 destination 1.1.1.1
#
 ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
```

Example: Configuring a GRE over IPv6 tunnel

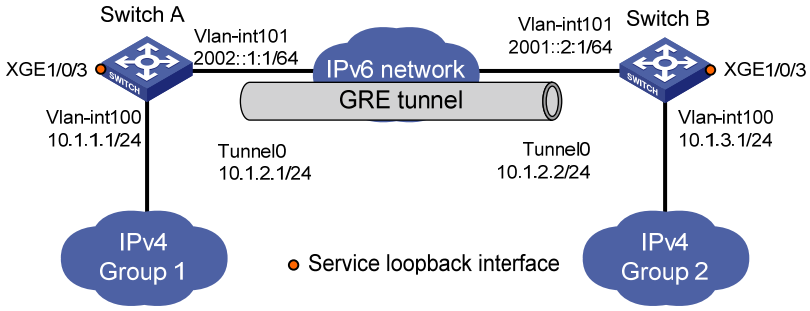
Applicable product matrix

Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 239, Switch A and Switch B can reach each other through IPv6. Configure a GRE tunnel between Switch A and Switch B so the two IPv4 networks Group 1 and Group 2 can reach each other over the IPv6 network.

Figure 239 Network diagram



Configuration procedures

Configuring Switch A

Specify an IPv4 address for VLAN-interface 100.

```
<SwitchA> system-view
[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 mode gre ipv6
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchA-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchA] interface Ten-GigabitEthernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IP network Group 2 through tunnel interface Tunnel 0.

```
[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] 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 mode gre ipv6
```

Specify an IPv4 address for the tunnel interface.

```
[SwitchB-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

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 Ten-GigabitEthernet 1/0/3 to service loopback group 1.

```
[SwitchB] interface Ten-GigabitEthernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure a static route to IP network Group 1 through tunnel interface Tunnel 0.

```
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

Verifying the configuration

Ping the IPv4 address of the peer interface VLAN-interface 100 from Switch B. The ping operation succeeds.

```
[SwitchB] ping -a 10.1.3.1 10.1.1.1
Ping 10.1.1.1 (10.1.1.1) from 10.1.3.1: 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=11.000 ms
56 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.000/2.400/11.000/4.317 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
 ipv6 address 2002::1:1/64
#
interface Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode gre ipv6
 ip address 10.1.2.1 255.255.255.0
 source 2002::1:1
 destination 2001::2:1
#
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
 ipv6 address 2001::2:1/64
#
interface Ten-GigabitEthernet1/0/3
 port service-loopback group 1
#
interface Tunnel0 mode gre ipv6
 ip address 10.1.2.2 255.255.255.0
 source 2001::2:1
 destination 2002::1:1
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel0
#
```

UDP helper configuration examples

This chapter provides UDP helper configuration examples.

Example: Configuring UDP helper

Applicable product matrix

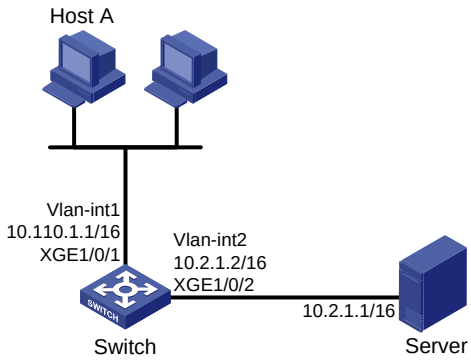
Product series	Software version
HP 5920	Release 2208P01
HP 5900	Release 2210

Network requirements

As shown in Figure 240, configure UDP helper on the switch to forward directed broadcast packets to the server at 10.2.1.1/16. The broadcast packets have the following details:

- Destination port number 55.
- Destination IP address 10.110.255.255.

Figure 240 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 interface 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 Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[Switch] interface ten-gigabitEthernet 1/0/2
[Switch-Ten-GigabitEthernet1/0/2] port access vlan 2
[Switch-Ten-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 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
```

Enable VLAN-interface 1 to receive directed broadcasts destined for the directly connected network.

```
[Switch-Vlan-interface1] ip forward-broadcast
```

Verifying the configuration

Display information about packets forwarded by UDP helper on VLAN-interface 1 destined for server 10.2.1.1.

```
[Switch-Vlan-interface1] display udp-helper interface vlan-interface 1
Interface         Server address       Packets sent
Vlan-interface1   10.2.1.1             5
```

Configuration files

```
#
 udp-helper enable
 udp-helper port 55
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 10.110.1.1 255.255.0.0
 ip forward-broadcast
 udp-helper server 10.2.1.1
#
```

```
interface Vlan-interface2
 ip address 10.2.1.2 255.255.0.0
#
interface Ten-GigabitEthernet1/0/1
#
interface Ten-GigabitEthernet1/0/2
port access vlan 2
#
```

uRPF configuration examples

This chapter provides Unicast Reverse Path Forwarding (uRPF) configuration examples.

Example: Configuring uRPF

Applicable product matrix

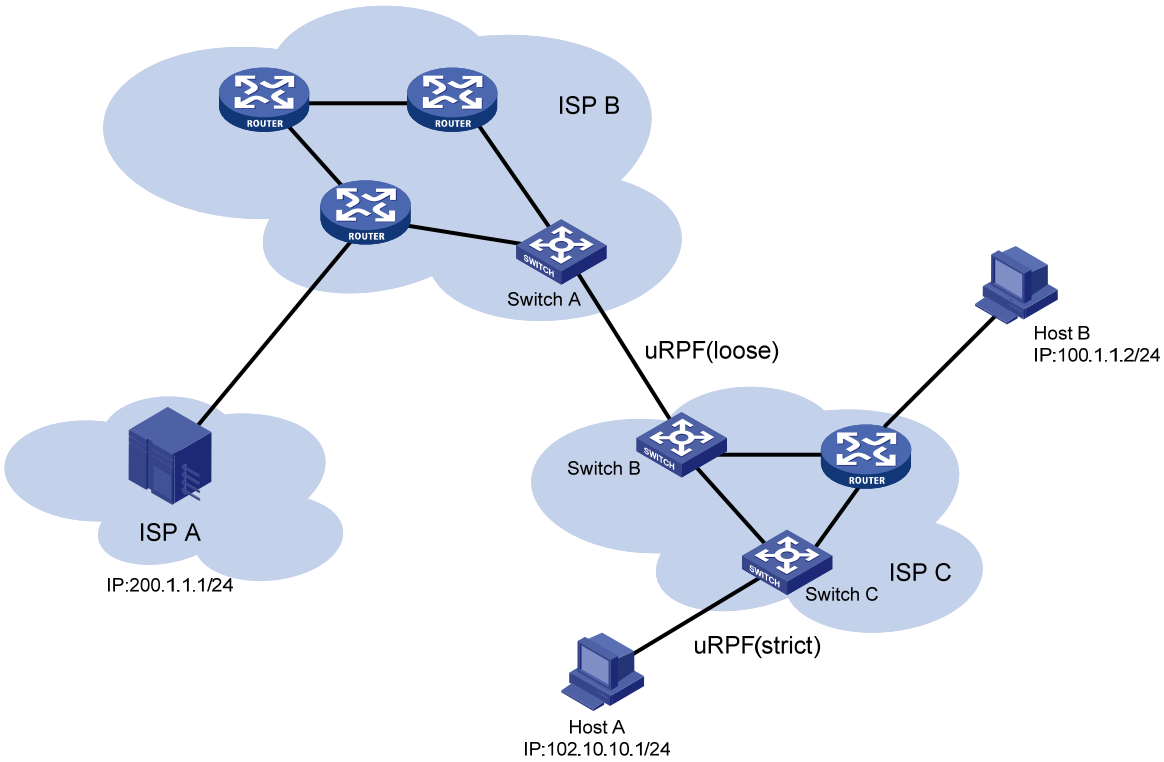
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 241:

- Enable loose uRPF on Switch A. This feature allows packets with source address matching the destination address of a FIB entry from ISP C network to pass.
- Enable strict uRPF on Switch C. This feature allows packets with source address and receiving interface matching the destination address and output interface of a FIB entry from Host A to pass.

Figure 241 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

1. Configure loose uRPF check.
```
<SwitchA> system-view
[SwitchA] ip urpf loose
```
2. Configure loose uRPF check.
```
<SwitchB> system-view
[SwitchB] ip urpf loose
```
3. Configure strict uRPF check.
```
<SwitchC> system-view
[SwitchC] ip urpf strict
```

Verifying the configuration

Send a packet with source IP address 100.1.1.2 and destination IP address 200.1.1.1 from Host A.

Capture packets on Host B. Host B does not receive any reply from IP address 200.1.1.1. This result indicates that strict uRPF functions. Switch C discards the packet with spoofed source IP address from Host A.

Configuration files

- Switch A:
```
#
 ip urpf loose
#
```
- Switch B:
```
#
 ip urpf loose
#
```
- Switch C:
```
#
 ip urpf strict
#
```

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 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

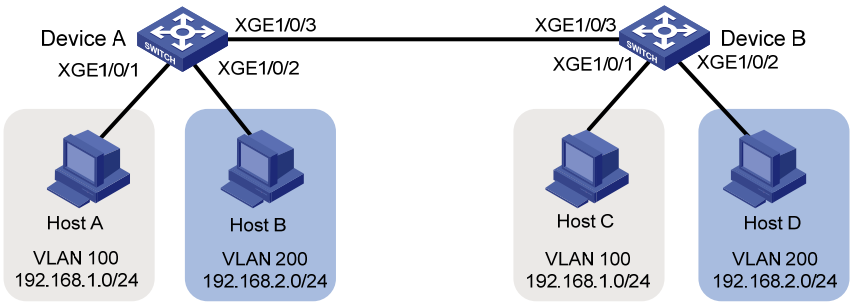
As shown in Figure 242:

- 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 to meet the following requirements:

- 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 242 Network diagram



Configuration procedures

Configuring Device A

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 to VLAN 100.

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

Create VLAN-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 Ten-GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceA] vlan 200
[DeviceA-vlan200] port ten-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 Ten-GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-type trunk
```

Assign Ten-GigabitEthernet 1/0/3 to VLAN 100 and VLAN 200.

```
[DeviceA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

Remove Ten-GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceA-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-Ten-GigabitEthernet1/0/3] quit
```

Configuring Device B

Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 to VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port ten-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 Ten-GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceB] vlan 200
[DeviceB-vlan200] port ten-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 Ten-GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port link-type trunk
```

Assign Ten-GigabitEthernet 1/0/3 to VLAN 100 and VLAN 200.

```
[DeviceB-Ten-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

Remove Ten-GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceB-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-Ten-GigabitEthernet1/0/3] quit
```

Verifying the configuration

1. Use the **display vlan** command to display the VLAN information and verify that 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:
    Ten-GigabitEthernet1/0/3
 Untagged Ports:
    Ten-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:
    Ten-GigabitEthernet1/0/3
 Untagged Ports:
    Ten-GigabitEthernet1/0/2
```

2. Ping Host A from Host C, ping Host C from Host A, and 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, an entry containing the IP address and MAC address of Host C exists.

- In the ARP table of Host C, an entry containing the IP address and MAC address of Host A exists.

3. Ping Host A from Host D, ping Host D from Host A, and 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 Ten-GigabitEthernet1/0/1
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 200
#
interface Ten-GigabitEthernet1/0/3
 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 Ten-GigabitEthernet1/0/1
 port access vlan 100
#
```

```
interface Ten-GigabitEthernet1/0/2
 port access vlan 200
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

VLAN tagging configuration examples

This chapter provides examples for using VLAN tagging features to extend customer VLANs (CVLANs) across an Ethernet service provider network.

VLAN tagging features enable service providers to separate or aggregate customer traffic in the service provider network. The following are available VLAN tagging operations:

- Adding a layer of service provider VLAN (SVLAN) tag.
- Modifying the SVLAN tag, CVLAN tag, or both.

The following are VLAN tagging features available for adding an SVLAN tag:

- **QinQ**—Tags all incoming frames (tagged or untagged) on the customer-side port with the PVID of the port.
- **One-to-two VLAN mapping**—Adds different SVLANs for traffic with different CVLAN tags.
- **Policy-based VLAN manipulation**—Uses a QoS policy to tag different classes of frames with different SVLAN tags. The traffic classifiers include CVLAN ID, IP address, and MAC address. In addition, you can configure the QoS policy to set the 802.1p priority in SVLAN tags.

The following are VLAN tagging features available for modifying VLAN tags:

- **VLAN mapping**—Includes the following features:
  - **One-to-one VLAN mapping**—Replaces one VLAN tag with another.
  - **Many-to-one VLAN mapping**—Replaces multiple VLAN tags with the same VLAN tag.
  - **Two-to-two VLAN mapping**—Replaces the SVLAN ID, CVLAN ID, or both IDs for an incoming double-tagged frame.
- **Policy-based VLAN manipulation**—Uses a QoS policy to modify the CVLAN or SVLAN ID by using the **remark customer-vlan-id** or **remark service-vlan-id** action. In addition, you can configure the QoS policy to set the 802.1p priority in SVLAN tags.

General configuration restrictions and guidelines

EVB and the VLAN tagging features are mutually exclusive. Do not enable EVB with any of these features on a port.

Example: Configuring QinQ

Applicable product matrix

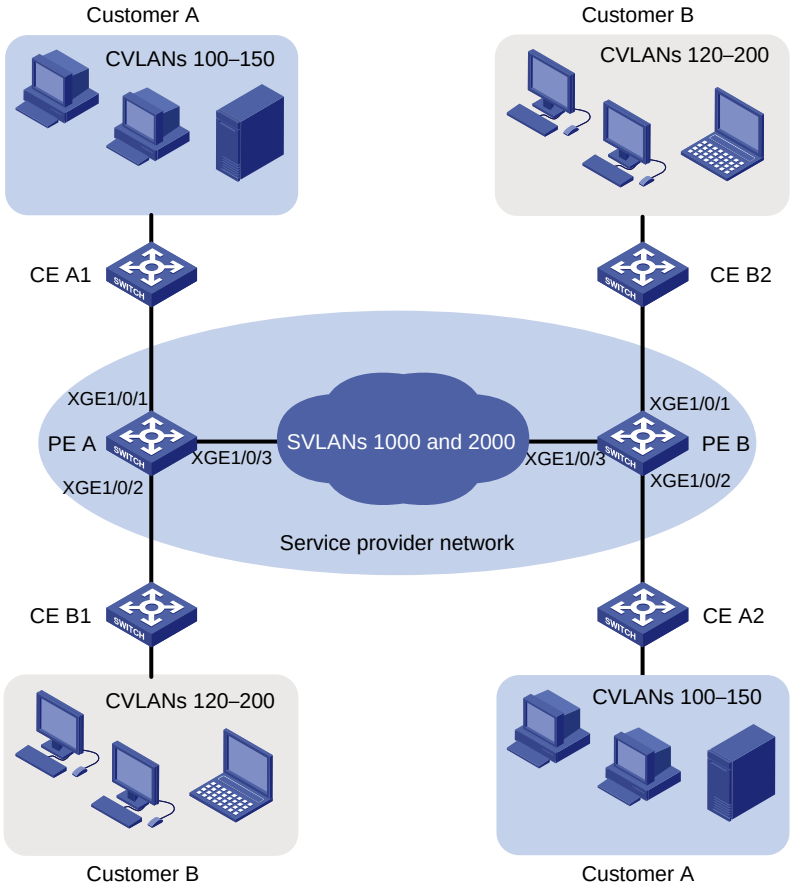
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 243, Customer A and Customer B each have two branches connected through a service provider network.

Configure QinQ on the service provider's PE A and PE B to transmit traffic of Customer A and Customer B in VLAN 1000 and VLAN 2000, respectively.

Figure 243 Network diagram



Requirements analysis

To run QinQ, you only need to configure QinQ on customer-side ports of PEs.

Configuration restrictions and guidelines

When you configure QinQ, follow these restrictions and guidelines:

- On the customer-side ports:
  - The link type of customer-side ports can be access, hybrid, or trunk. Whichever link type you choose, QinQ tags incoming frames (tagged or untagged) with the PVID tag.
  - If the link type is trunk or hybrid, you must set the SVLAN ID as the PVID. For a hybrid customer-side port to send traffic to the customer site with the SVLAN tag removed, you must also assign the port to the SVLAN as an untagged VLAN member.

- For the service provider-side ports to support multiple SVLANs, you must configure their link type as trunk or hybrid.
- For QinQ frames to travel across the service provider network, you must perform the following tasks:
  - Increase the MTU to at least 1504 bytes for each port on the path of QinQ frames.
  - Configure all the ports on the forwarding path to allow frames from VLANs 1000 and 2000 to pass through without removing the VLAN tag.

Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

Configuring PE A

1. Create VLANs 1000 and 2000.

```
<PE_A> system-view
[PE_A] vlan 1000
[PE_A-vlan1000] quit
[PE_A] vlan 2000
[PE_A-vlan2000] quit
```

2. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port, and set its PVID to 1000.

```
[PE_A] interface ten-gigabitethernet 1/0/1
[PE_A-Ten-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-Ten-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-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
[PE_A-Ten-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

   # Enable QinQ on the port.

```
[PE_A-Ten-GigabitEthernet1/0/1] qinq enable
[PE_A-Ten-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

   # Configure the port as an access port, and assign it to VLAN 2000.

```
[PE_A] interface ten-gigabitethernet 1/0/2
[PE_A-Ten-GigabitEthernet1/0/2] port access vlan 2000
```

   # Enable QinQ on the port.

```
[PE_A-Ten-GigabitEthernet1/0/2] qinq enable
[PE_A-Ten-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port Ten-GigabitEthernet 1/0/3:

   # Configure the port as a trunk port, and assign it to VLANs 1000 and 2000.

```
[PE_A] interface ten-gigabitethernet 1/0/3
[PE_A-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE_A-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

   # Remove the port from VLAN 1.

```
[PE_A-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_A-Ten-GigabitEthernet1/0/3] quit
```

Configuring PE B

1. Create VLANs 1000 and 2000.

```
<PE_B> system-view
[PE_B] vlan 1000
[PE_B-vlan1000] quit
[PE_B] vlan 2000
[PE_B-vlan2000] quit
```

2. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port, and set its PVID to 2000.

```
[PE_B] interface ten-gigabitethernet 1/0/1
[PE_B-Ten-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-Ten-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-Ten-GigabitEthernet1/0/1] port hybrid vlan 2000 untagged
[PE_B-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Enable QinQ on the port.

```
[PE_B-Ten-GigabitEthernet1/0/1] qinq enable
[PE_B-Ten-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

   # Configure the port as an access port, and assign it to VLAN 1000.

```
[PE_B] interface ten-gigabitethernet 1/0/2
[PE_B-Ten-GigabitEthernet1/0/2] port access vlan 1000
```

   # Enable QinQ on the port.

```
[PE_B-Ten-GigabitEthernet1/0/2] qinq enable
[PE_B-Ten-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port Ten-GigabitEthernet 1/0/3:

   # Configure the port as a trunk port, and assign it to VLANs 1000 and 2000.

```
[PE_B] interface ten-gigabitethernet 1/0/3
[PE_B-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE_B-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

   # Remove the port from VLAN 1.

```
[PE_B-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_B-Ten-GigabitEthernet1/0/3] quit
```

Configuring devices in the service provider network

Make sure all ports on the path between PE A and PE B allow frames from VLANs 1000 and 2000 to pass through without removing the VLAN tag. (Details not shown.)

Verifying the configuration

Verify the configuration on each port. This example uses Ten-GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface ten-gigabitethernet 1/0/1
[PE_A-Ten-GigabitEthernet1/0/1] display this
#
interface ten-gigabitethernet1/0/1
 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 ten-gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
interface ten-gigabitethernet1/0/2
 port access vlan 2000
 qinq enable
#
interface ten-gigabitethernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
#
```

- PE B:

```
#
vlan 1000
#
vlan 2000
#
interface ten-gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2000 untagged
 port hybrid pvid vlan 2000
 qinq enable
#
interface ten-gigabitethernet1/0/2
 port access vlan 1000
 qinq enable
#
```

```
interface ten-gigabitethernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
#
```

Example: Configuring one-to-two VLAN mapping

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 244:

- 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. For each customer, the service provider assigns one SVLAN by traffic type.

Configure one-to-two VLAN mappings on each customer-side port of PE A and PE B to separate the traffic by customer and traffic type. In the SVLAN tag, use the same 802.1p priority as the CVLAN tag.

Figure 244 Network diagram

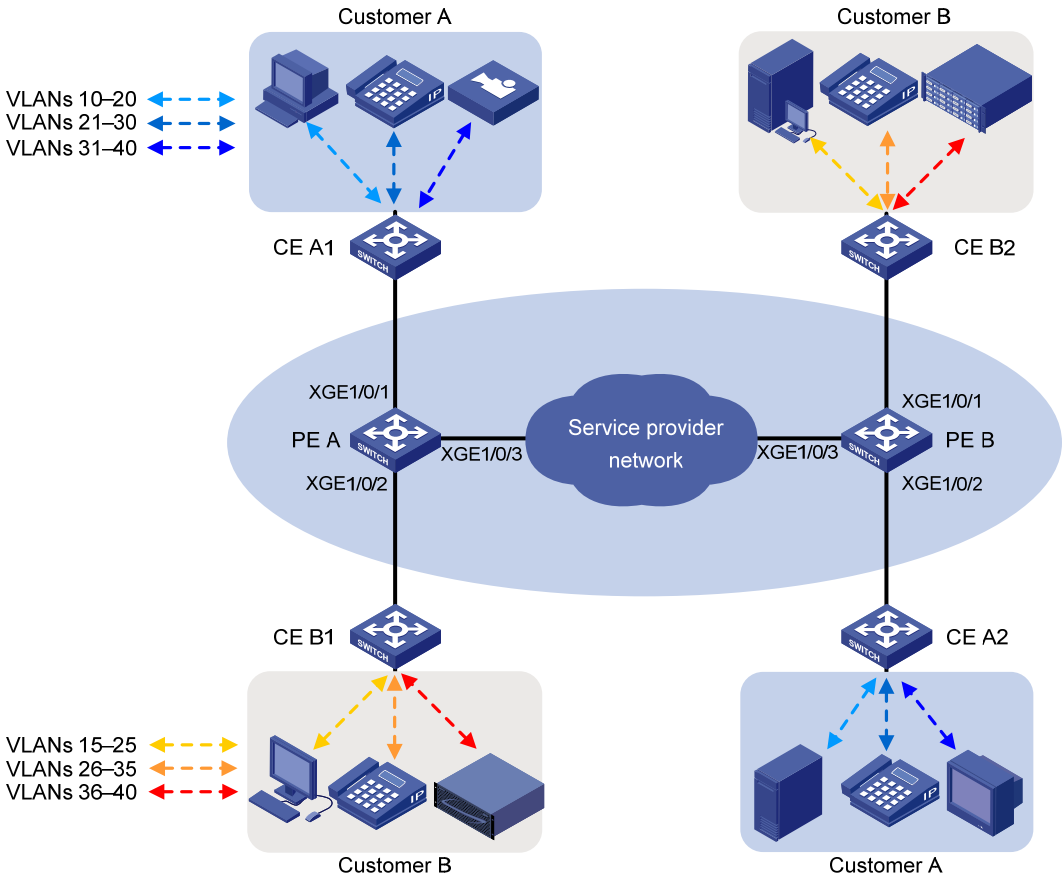
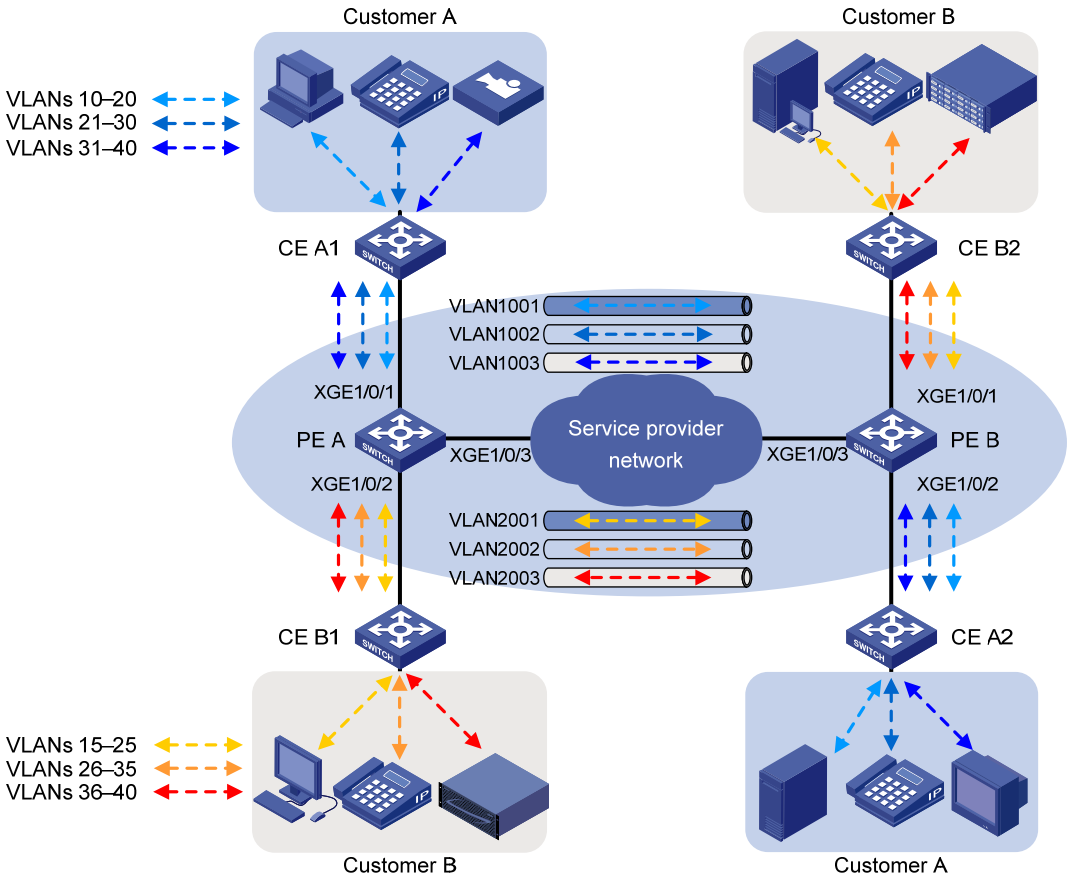


Table 25 shows the VLAN mapping table. Figure 245 shows the traffic transmission pattern after the one-to-two VLAN mappings are configured on customer-side ports.

Table 25 VLAN mapping table

Traffic type	CVLANs	SVLAN
Customer A:		
Video	31 to 40	1003
Voice	21 to 30	1002
Data	10 to 20	1001
Customer B:		
Storage	36 to 40	2003
Voice	26 to 35	2002
Data	15 to 25	2001

Figure 245 Traffic pattern in the service provider network after one-to-two VLAN mapping is configured



Requirements analysis

For the customer-side ports to support multiple SVLANs and send traffic to the customer site with the SVLAN tag removed, you must perform the following tasks:

1. Configure the link type of the customer-side ports as hybrid.
2. Assign the ports to the SVLANs as untagged VLAN members.

For the SVLAN tag to use the same 802.1p priority as the CVLAN tag, you must configure the customer-side port to trust the priority mode on the port. By default, the 802.1p priority in the SVLAN tag depends on the priority trust mode on the port.

- If the 802.1p priority in frames is trusted, the device copies the 802.1p priority in the CVLAN tag to the SVLAN tag.
- If port priority is trusted, the port priority is used as the 802.1p priority in the SVLAN tag. For untagged incoming frames, the port encapsulates the port priority as the 802.1p priority in the SVLAN tag.

Configuration restrictions and guidelines

When you configure one-to-two VLAN mappings, follow these restrictions and guidelines:

- If QinQ is also enabled on the customer-side port, one-to-two VLAN mappings have priority over QinQ.
  - Frames that match a one-to-two VLAN mapping are tagged with the SVLAN tag in the mapping.
  - Frames that do not match any one-to-two VLAN mapping are tagged with the PVID tag.
- For double-tagged frames to travel across the service provider network, you must perform the following tasks:
  - Increase the MTU to at least 1504 bytes for each port on the path of double-tagged frames.
  - Configure all the ports on the forwarding path to allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through without removing the VLAN tag.

Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

Configuring PE A

1. Create CVLANs 10 to 40.

```
<PE_A> system-view
[PE_A] vlan 10 to 40
```

2. Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_A] vlan 1001 to 1003
[PE_A] vlan 2001 to 2003
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port.

```
[PE_A] interface ten-gigabitethernet 1/0/1
[PE_A-Ten-GigabitEthernet1/0/1] port link-type hybrid
```

   # Assign the port to CVLANs 10 through 40 as a tagged VLAN member.

```
[PE_A-Ten-GigabitEthernet1/0/1] port hybrid vlan 10 to 40 tagged
```

   # Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_A-Ten-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
```

   # Remove the port from VLAN 1.

```
[PE_A-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Configure a one-to-two VLAN mapping to add SVLAN tag 1001 to traffic from VLANs 10 through 20.

```
[PE_A-Ten-GigabitEthernet1/0/1] vlan mapping nest range 10 to 20 nested-vlan 1001
```

   # Configure a one-to-two VLAN mapping to add SVLAN tag 1002 to traffic from VLANs 21 through 30.

```
[PE_A-Ten-GigabitEthernet1/0/1] vlan mapping nest range 21 to 30 nested-vlan 1002
```

   # Configure a one-to-two VLAN mapping to add SVLAN tag 1003 to traffic from VLANs 31 through 40.

```
[PE_A-Ten-GigabitEthernet1/0/1] vlan mapping nest range 31 to 40 nested-vlan 1003
```

   # Configure the port to trust the 802.1p priority of frames.

```
[PE_A-Ten-GigabitEthernet1/0/1] qos trust dot1p
[PE_A-Ten-GigabitEthernet1/0/1] quit
```

4. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

Configure the port as a hybrid port.

```
[PE_A] interface ten-gigabitethernet 1/0/2
[PE_A-Ten-GigabitEthernet1/0/2] port link-type hybrid
```

Assign the port to CVLANs 15 through 40 as a tagged VLAN member.

```
[PE_A-Ten-GigabitEthernet1/0/2] port hybrid vlan 15 to 40 tagged
```

Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_A-Ten-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
```

Remove the port from VLAN 1.

```
[PE_A-Ten-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Configure a one-to-two VLAN mapping to add SVLAN tag 2001 to traffic from VLANs 15 through 25.

```
[PE_A-Ten-GigabitEthernet1/0/2] vlan mapping nest range 15 to 25 nested-vlan 2001
```

Configure a one-to-two VLAN mapping to add SVLAN tag 2002 to traffic from VLANs 26 through 35.

```
[PE_A-Ten-GigabitEthernet1/0/2] vlan mapping nest range 26 to 35 nested-vlan 2002
```

Configure a one-to-two VLAN mapping to add SVLAN tag 2003 to traffic from VLANs 36 through 40.

```
[PE_A-Ten-GigabitEthernet1/0/2] vlan mapping nest range 36 to 40 nested-vlan 2003
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_A-Ten-GigabitEthernet1/0/2] qos trust dot1p
[PE_A-Ten-GigabitEthernet1/0/2] quit
```

5. Configure the service provider-side port Ten-GigabitEthernet 1/0/3:

Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_A] interface ten-gigabitethernet 1/0/3
[PE_A-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE_A-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_A-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_A-Ten-GigabitEthernet1/0/3] quit
```

Configuring PE B

1. Create CVLANs 10 to 40.

```
<PE_B> system-view
[PE_B] vlan 10 to 40
```

2. Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B] vlan 1001 to 1003
[PE_B] vlan 2001 to 2003
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

Configure the port as a hybrid port.

```
[PE_B] interface ten-gigabitethernet 1/0/1
[PE_B-Ten-GigabitEthernet1/0/1] port link-type hybrid
```

Assign the port to CVLANs 15 through 40 as a tagged VLAN member.

```
[PE_B-Ten-GigabitEthernet1/0/1] port hybrid vlan 15 to 40 tagged
```

Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_B-Ten-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

Remove the port from VLAN 1.

```
[PE_B-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Configure a one-to-two VLAN mapping to add SVLAN tag 2001 to traffic from VLANs 15 through 25.

```
[PE_B-Ten-GigabitEthernet1/0/1] vlan mapping nest range 15 to 25 nested-vlan 2001
```

Configure a one-to-two VLAN mapping to add SVLAN tag 2002 to traffic from VLANs 26 through 35.

```
[PE_B-Ten-GigabitEthernet1/0/1] vlan mapping nest range 26 to 35 nested-vlan 2002
```

Configure a one-to-two VLAN mapping to add SVLAN tag 2003 to traffic from VLANs 36 through 40.

```
[PE_B-Ten-GigabitEthernet1/0/1] vlan mapping nest range 36 to 40 nested-vlan 2003
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_B-Ten-GigabitEthernet1/0/1] qos trust dot1p
[PE_B-Ten-GigabitEthernet1/0/1] quit
```

4. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

Configure the port as a hybrid port.

```
[PE_B] interface ten-gigabitethernet 1/0/2
[PE_B-Ten-GigabitEthernet1/0/2] port link-type hybrid
```

Assign the port to CVLANs 10 through 40 as a tagged VLAN member.

```
[PE_B-Ten-GigabitEthernet1/0/2] port hybrid vlan 10 to 40 tagged
```

Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_B-Ten-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
```

Remove the port from VLAN 1.

```
[PE_B-Ten-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Configure a one-to-two VLAN mapping to add SVLAN tag 1001 to traffic from VLANs 10 through 20.

```
[PE_B-Ten-GigabitEthernet1/0/2] vlan mapping nest range 10 to 20 nested-vlan 1001
```

Configure a one-to-two VLAN mapping to add SVLAN tag 1002 to traffic from VLANs 21 through 30.

```
[PE_B-Ten-GigabitEthernet1/0/2] vlan mapping nest range 21 to 30 nested-vlan 1002
```

Configure a one-to-two VLAN mapping to add SVLAN tag 1003 to traffic from VLANs 31 through 40.

```
[PE_B-Ten-GigabitEthernet1/0/2] vlan mapping nest range 31 to 40 nested-vlan 1003
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_B-Ten-GigabitEthernet1/0/2] qos trust dot1p
[PE_B-Ten-GigabitEthernet1/0/2] quit
```

5. Configure the service provider-side port Ten-GigabitEthernet 1/0/3:

Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_B] interface ten-gigabitethernet 1/0/3
[PE_B-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE_B-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-Ten-GigabitEthernet1/0/3] quit
```

Configuring devices in the service provider network

Make sure all ports on the path between PE A and PE B allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through without removing the VLAN tag. (Details not shown.)

Verifying the configuration

Verify the VLAN mappings on PE A.

```
[PE_A] display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10-20         N/A           1001                     10-20
  21-30         N/A           1002                     21-30
  31-40         N/A           1003                     31-40
Interface Ten-GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  15-25         N/A           2001                     15-25
  26-35         N/A           2002                     26-35
  36-40         N/A           2003                     36-40
```

Verify the VLAN mappings on PE B.

```
[PE_B] display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  15-25         N/A           2001                     15-25
  26-35         N/A           2002                     26-35
  36-40         N/A           2003                     36-40
Interface Ten-GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10-20         N/A           1001                     10-20
  21-30         N/A           1002                     21-30
  31-40         N/A           1003                     31-40
```

Configuration files

- PE A:

```
#
vlan 10 to 40
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
interface Ten-GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 to 40 tagged
 port hybrid vlan 1001 to 1003 untagged
 vlan mapping nest range 10 to 20 nested-vlan 1001
```

```
 vlan mapping nest range 21 to 30 nested-vlan 1002
 vlan mapping nest range 31 to 40 nested-vlan 1003
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 15 to 40 tagged
 port hybrid vlan 2001 to 2003 untagged
 vlan mapping nest range 15 to 25 nested-vlan 2001
 vlan mapping nest range 26 to 35 nested-vlan 2002
 vlan mapping nest range 36 to 40 nested-vlan 2003
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

- PE B:

```
#
vlan 10 to 40
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
interface Ten-GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 15 to 40 tagged
 port hybrid vlan 2001 to 2003 untagged
 vlan mapping nest range 15 to 25 nested-vlan 2001
 vlan mapping nest range 26 to 35 nested-vlan 2002
 vlan mapping nest range 36 to 40 nested-vlan 2003
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 to 40 tagged
 port hybrid vlan 1001 to 1003 untagged
 vlan mapping nest range 10 to 20 nested-vlan 1001
 vlan mapping nest range 21 to 30 nested-vlan 1002
 vlan mapping nest range 31 to 40 nested-vlan 1003
 qos trust dot1p
#
interface Ten-GigabitEthernet1/0/3
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

Example: Configuring QoS policies for SVLAN tagging and 802.1p priority re-marking

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 246:

- 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.

Apply a QoS policy to each customer-side port 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 246 Network diagram

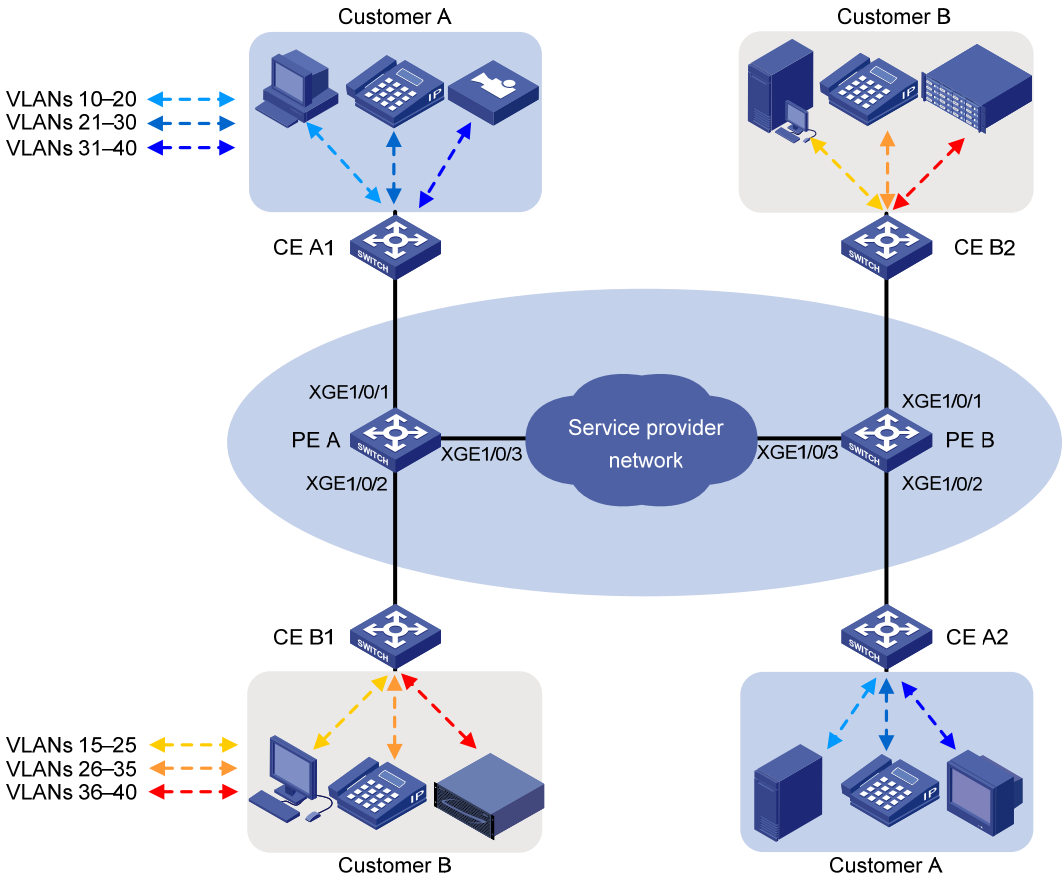
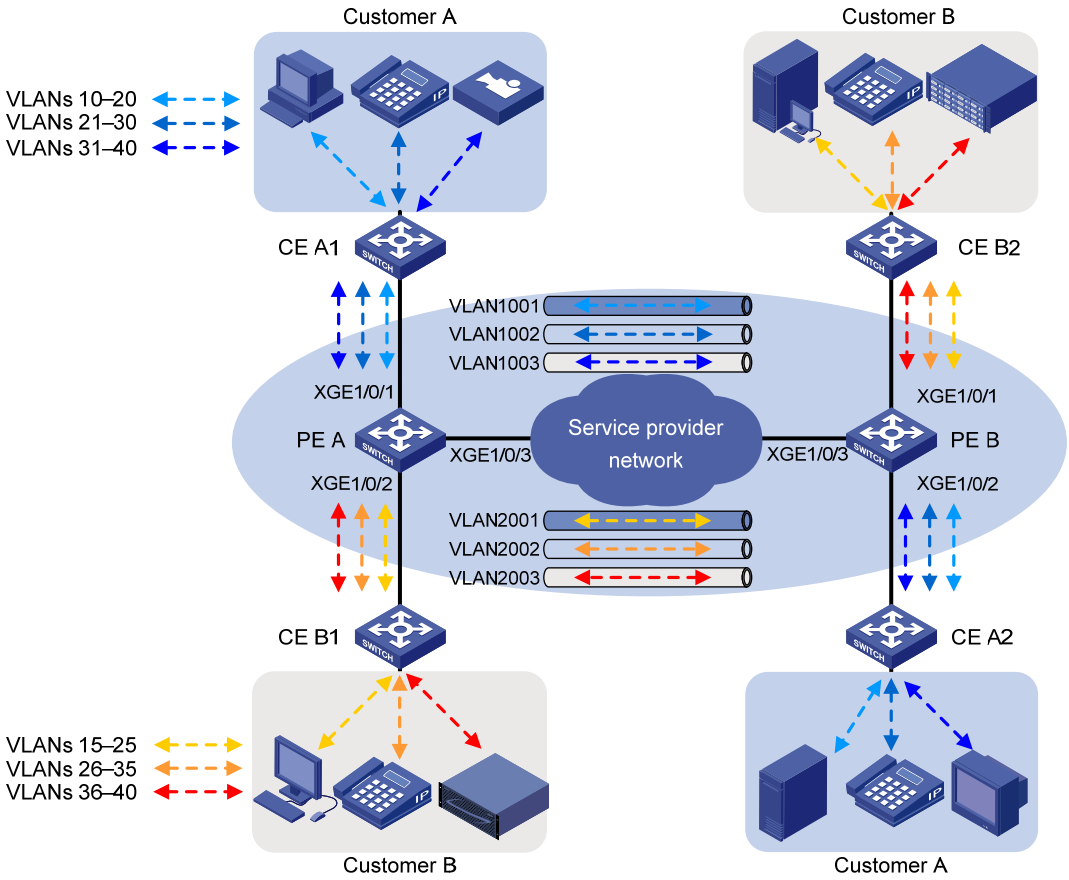


Table 26 shows the VLAN and 802.1p priority assignment scheme. For each customer, the service provider assigns one SVLAN by traffic type. Figure 247 shows the traffic transmission pattern after the QoS policies are applied to customer-side ports.

Table 26 VLAN and traffic priority 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 247 Traffic pattern in the service provider network after QoS policies are applied



Requirements analysis

For the customer-side ports to support multiple SVLANs and send traffic to the customer site with the SVLAN tag removed, you must perform the following tasks:

1. Configure the link type of the customer-side ports as hybrid.
2. Assign the ports to the SVLANs as untagged VLAN members.

To change the 802.1p priority for a class of traffic, use the **remark dot1p** action. By default, the 802.1p priority in the SVLAN tag added by a QinQ-enabled port depends on the priority trust mode on the port.

- If the 802.1p priority in frames is trusted, the device copies the 802.1p priority in the CVLAN tag to the SVLAN tag.
- If port priority is trusted, the port priority is used as the 802.1p priority in the SVLAN tag. For untagged incoming frames, the port encapsulates the port priority as the 802.1p priority in the SVLAN tag.

Configuration restrictions and guidelines

When you configure a SVLAN tagging QoS policy, follow these restrictions and guidelines:

- Use the **nest** action for SVLAN tagging. You can configure only one nest action in the traffic behavior for a traffic class.

- You must apply the QoS policy to the inbound direction of customer-side ports.
- For the nest action to take effect, you must enable QinQ on the customer-side ports.
- If an incoming frame does not match the QoS policy, the port adds the PVID tag to the frame as the SVLAN tag.

For QinQ frames to travel across the service provider network, follow these restrictions and guidelines:

- Increase the MTU to at least 1504 bytes for each port on the path of QinQ frames.
- Configure all the ports on the forwarding path to allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through without removing the VLAN tag.

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 SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
<PE_A> system-view
[PE_A] vlan 1001 to 1003
[PE_A] vlan 2001 to 2003
```

2. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface ten-gigabitethernet 1/0/1
[PE_A-Ten-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_A-Ten-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
```

   # Enable QinQ on the port.

```
[PE_A-Ten-GigabitEthernet1/0/1] qinq enable
```

   # Configure the port to trust the 802.1p priority of frames.

```
[PE_A-Ten-GigabitEthernet1/0/1] qos trust dot1p
[PE_A-Ten-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

   # Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface ten-gigabitethernet 1/0/2
[PE_A-Ten-GigabitEthernet1/0/2] port link-type hybrid
[PE_A-Ten-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

   # Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_A-Ten-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
```

   # Enable QinQ on the port.

```
[PE_A-Ten-GigabitEthernet1/0/2] qinq enable
```

   # Configure the port to trust the 802.1p priority of frames.

```
[PE_A-Ten-GigabitEthernet1/0/2] qos trust dot1p
[PE_A-Ten-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port Ten-GigabitEthernet 1/0/3:

   # Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_A] interface ten-gigabitethernet 1/0/3
[PE_A-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE_A-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

   # Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_A-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_A-Ten-GigabitEthernet1/0/3] quit
```

5. Configure QoS policies for SVLAN tagging and 802.1p priority re-mark:

   # Create the class **customer_A_pc** to match traffic from CVLANs 10 through 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 and 802.1p priority re-mark actions for Customer A's three traffic types.

```
[PE_A] traffic behavior customer_A_pc
[PE_A-behavior-customer_A_pc] nest top-most vlan 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 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 1003
[PE_A-behavior-customer_A_video] remark dot1p 7
[PE_A-behavior-customer_A_video] quit
```

   # Create the QoS policy **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 Ten-GigabitEthernet 1/0/1.

```
[PE_A] interface ten-gigabitethernet 1/0/1
[PE_A-Ten-GigabitEthernet1/0/1] qos apply policy customer_A inbound
[PE_A-Ten-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 and 802.1p priority re-mark behaviors for Customer B's traffic types.

```
[PE_A] traffic behavior customer_B_pc
[PE_A-behavior-customer_B_pc] nest top-most vlan 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 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 2003
[PE_A-behavior-customer_B_storage] remark dot1p 7
[PE_A-behavior-customer_B_storage] quit
```

Create the QoS policy **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 Ten-GigabitEthernet 1/0/2.

```
[PE_A] interface ten-gigabitethernet 1/0/2
[PE_A-Ten-GigabitEthernet1/0/2] qos apply policy customer_B inbound
[PE_A-Ten-GigabitEthernet1/0/2] quit
```

Configuring PE B

1. Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
<PE_B> system-view
[PE_B] vlan 1001 to 1003
[PE_B] vlan 2001 to 2003
```

2. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface ten-gigabitethernet 1/0/1
[PE_B-Ten-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_B-Ten-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

Enable QinQ on the port.

```
[PE_B-Ten-GigabitEthernet1/0/1] qinq enable
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_B-Ten-GigabitEthernet1/0/1] qos trust dot1p
[PE_B-Ten-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface ten-gigabitethernet 1/0/2
[PE_B-Ten-GigabitEthernet1/0/2] port link-type hybrid
[PE_B-Ten-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_B-Ten-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
```

Enable QinQ on the port.

```
[PE_B-Ten-GigabitEthernet1/0/2] qinq enable
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_B-Ten-GigabitEthernet1/0/2] qos trust dot1p
[PE_B-Ten-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port Ten-GigabitEthernet 1/0/3:

Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_B] interface ten-gigabitethernet 1/0/3
[PE_B-Ten-GigabitEthernet1/0/3] port link-type trunk
[PE_B-Ten-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-Ten-GigabitEthernet1/0/3] quit
```

5. Configure QoS policies for SVLAN tagging and 802.1p priority re-mark:

#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 and 802.1p priority re-mark behaviors for Customer A's three traffic types.

```
[PE_B] traffic behavior customer_A_pc
[PE_B-behavior-customer_A_pc] nest top-most vlan 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 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 1003
[PE_B-behavior-customer_A_video] remark dot1p 7
[PE_B-behavior-customer_A_video] quit
```

Create the QoS policy **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 the QoS policy **customer_A** to the inbound direction of Ten-GigabitEthernet 1/0/2.

```
[PE_B] interface ten-gigabitethernet 1/0/2
[PE_B-Ten-GigabitEthernet1/0/2] qos apply policy customer_A inbound
[PE_B-Ten-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 and 802.1p priority re-mark behaviors for Customer B's three traffic types.

```
[PE_B] traffic behavior customer_B_pc
[PE_B-behavior-customer_B_pc] nest top-most vlan 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 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 2003
[PE_B-behavior-customer_B_storage] remark dot1p 7
[PE_B-behavior-customer_B_storage] quit
```

Create the QoS policy **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 Ten-GigabitEthernet 1/0/1.

```
[PE_B] interface ten-gigabitethernet 1/0/1
[PE_B-Ten-GigabitEthernet1/0/1] qos apply policy customer_B inbound
[PE_B-Ten-GigabitEthernet1/0/1] quit
```

Configuring devices in the service provider network

Make sure all ports on the path between PE A and PE B allow frames from VLANs 1001 through 1003 and VLANs 2001 through 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. This example uses Ten-GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface ten-gigabitethernet 1/0/1
[PE_A-Ten-GigabitEthernet1/0/1] display this
#
interface ten-gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_A inbound
#
Return
[PE_A-Ten-GigabitEthernet1/0/1] quit
```

Use the **display qos policy interface** command to verify the QoS configuration on each port. This example uses Ten-GigabitEthernet 1/0/1 of PE A.

```
[PE_A] display qos policy interface ten-gigabitethernet 1/0/1
Interface: Ten-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 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 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 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 1001
 remark dot1p 3
#
traffic behavior customer_A_voice
 nest top-most vlan 1002
 remark dot1p 5
#
traffic behavior customer_A_video
 nest top-most vlan 1003
 remark dot1p 7
```

```
#
traffic behavior customer_B_pc
 nest top-most vlan 2001
 remark dot1p 3
#
traffic behavior customer_B_voice
 nest top-most vlan 2002
 remark dot1p 5
#
traffic behavior customer_B_storage
 nest top-most vlan 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 ten-gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_A inbound
#
interface ten-gigabitethernet1/0/2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_B inbound
#
interface ten-gigabitethernet1/0/3
 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 1001
 remark dot1p 3
#
traffic behavior customer_A_voice
 nest top-most vlan 1002
 remark dot1p 5
#
traffic behavior customer_A_video
 nest top-most vlan 1003
 remark dot1p 7
#
traffic behavior customer_B_pc
 nest top-most vlan 2001
 remark dot1p 3
#
traffic behavior customer_B_voice
 nest top-most vlan 2002
 remark dot1p 5
#
traffic behavior customer_B_storage
 nest top-most vlan 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 ten-gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_B inbound
#
interface ten-gigabitethernet1/0/2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_A inbound
#
interface ten-gigabitethernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

Example: Configuring one-to-one and many-to-one VLAN mappings

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 248:

- Each household subscribes to PC, VoD, and VoIP services, and obtains the IP address through DHCP.
- On the home gateways, VLANs 1, 2, and 3 are assigned to PC, VoD, and VoIP traffic, respectively.

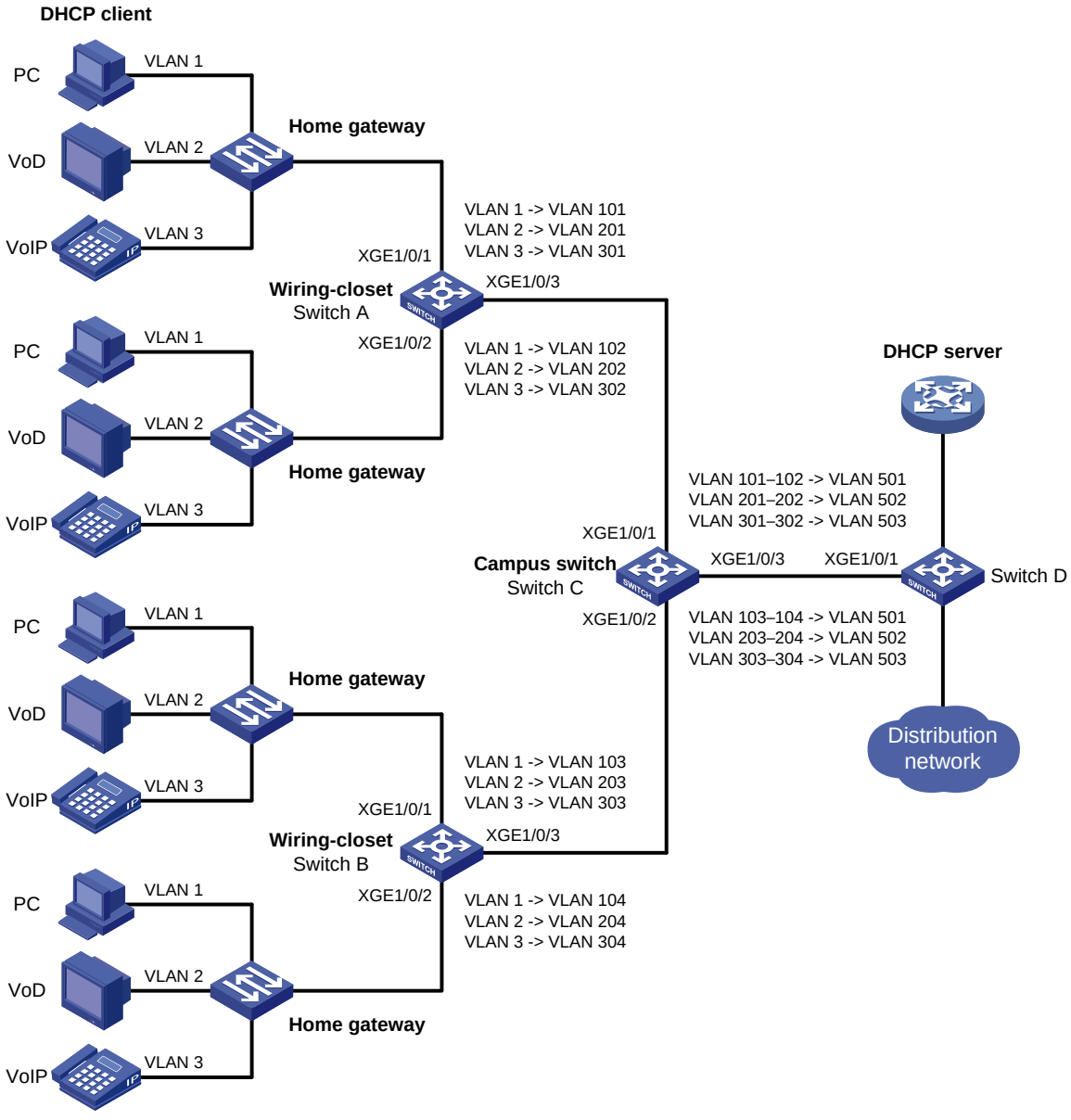
To isolate traffic of the same service type from different households, configure one-to-one VLAN mappings on the wiring-closet switches to assign one VLAN to each type of traffic from each household.

To save VLAN resources, configure many-to-one VLAN mappings on the campus switch (Switch C) to transmit the same type of traffic from different households in one VLAN. Use VLANs 501, 502, and 503 for PC, VoD, and VoIP traffic, respectively.

Table 27 VLAN mappings for each service

Service	VLANs on home gateways	VLANs on wiring-closet switches (Switch A and Switch B)	VLANs on campus switch (Switch C)
PC	VLAN 1	VLANs 101, 102, 103, 104	VLAN 501
VoD	VLAN 2	VLANs 201, 202, 203, 204	VLAN 502
VoIP	VLAN 3	VLANs 301, 302, 303, 304	VLAN 503

Figure 248 Network diagram



Configuration procedure

Configuring Switch A

Create the original VLANs.

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
```

Create the translated VLANs.

```
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

Configure the customer-side port Ten-GigabitEthernet 1/0/1 as a trunk port. Assign the port to all original VLANs and translated VLANs.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301
```

Configure one-to-one VLAN mappings on Ten-GigabitEthernet 1/0/1 to map VLANs 1, 2, and 3 to VLANs 101, 201, and 301, respectively.

```
[SwitchA-Ten-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
[SwitchA-Ten-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201
[SwitchA-Ten-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Configure the customer-side port Ten-GigabitEthernet 1/0/2 as a trunk port. Assign the port to all original VLANs and translated VLANs.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302
```

Configure one-to-one VLAN mappings on Ten-GigabitEthernet 1/0/2 to map VLANs 1, 2, and 3 to VLANs 102, 202, and 302, respectively.

```
[SwitchA-Ten-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102
[SwitchA-Ten-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202
[SwitchA-Ten-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Configure the network-side port Ten-GigabitEthernet 1/0/3 as a trunk port. Assign the port to the translated VLANs.

```
[SwitchA] interface ten-gigabitethernet 1/0/3
[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
[SwitchA-Ten-GigabitEthernet1/0/3] quit
```

Configuring Switch B

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

Configuring Switch C

1. Configure the basic settings required for many-to-one VLAN mappings:

   # Enable DHCP snooping.

   ```
   <SwitchC> system-view
   ```

```
[SwitchC] dhcp snooping enable
```

Create the original VLANs and translated VLANs, and enable ARP detection for these VLANs.

```
[SwitchC] vlan 101
[SwitchC-vlan101] arp detection enable
[SwitchC-vlan101] vlan 201
[SwitchC-vlan201] arp detection enable
[SwitchC-vlan201] vlan 301
[SwitchC-vlan301] arp detection enable
[SwitchC-vlan301] vlan 102
[SwitchC-vlan102] arp detection enable
[SwitchC-vlan102] vlan 202
[SwitchC-vlan202] arp detection enable
[SwitchC-vlan202] vlan 302
[SwitchC-vlan302] arp detection enable
[SwitchC-vlan302] vlan 103
[SwitchC-vlan103] arp detection enable
[SwitchC-vlan103] vlan 203
[SwitchC-vlan203] arp detection enable
[SwitchC-vlan203] vlan 303
[SwitchC-vlan303] arp detection enable
[SwitchC-vlan303] vlan 104
[SwitchC-vlan104] arp detection enable
[SwitchC-vlan104] vlan 204
[SwitchC-vlan204] arp detection enable
[SwitchC-vlan204] vlan 304
[SwitchC-vlan304] arp detection enable
[SwitchC-vlan304] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan501] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan502] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit
```

2. Configure the customer-side port Ten-GigabitEthernet 1/0/1:

Configure the port as a trunk port. Assign the port to the original VLANs and translated VLANs.

```
[SwitchC] interface ten-gigabitethernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 101 102 201 202 301 302 501
to 503
```

Configure the user-side many-to-one VLAN mappings to map VLANs for PC, VoD, and VoIP traffic to VLANs 501, 502, and 503, respectively.

```
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping uni range 101 to 102 translated-vlan
501
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping uni range 201 to 202 translated-vlan
502
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping uni range 301 to 302 translated-vlan
503
```

Enable DHCP snooping entry recording.

```
[SwitchC-Ten-GigabitEthernet1/0/1] dhcp snooping binding record
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port Ten-GigabitEthernet 1/0/2:

   # Configure the port as a trunk port. Assign the port to the original VLANs and translated VLANs.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 103 104 203 204 303 304 501
to 503
```

   # Configure the user-side many-to-one VLAN mappings to map VLANs for PC, VoD, and VoIP traffic to VLANs 501, 502, and 503, respectively.

```
[SwitchC-Ten-GigabitEthernet1/0/2] vlan mapping uni range 103 to 104 translated-vlan
501
[SwitchC-Ten-GigabitEthernet1/0/2] vlan mapping uni range 203 to 204 translated-vlan
502
[SwitchC-Ten-GigabitEthernet1/0/2] vlan mapping uni range 303 to 304 translated-vlan
503
```

   # Enable DHCP snooping entry recording.

```
[SwitchC-Ten-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

4. Configure the network-side port Ten-GigabitEthernet 1/0/3:

   # Enable the network-side VLAN mapping function on the port.

```
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] vlan mapping nni
```

   # Configure the port as a trunk port. Assign the port to the translated VLANs 501 through 503.

```
[SwitchC-Ten-GigabitEthernet1/0/3] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/3] port trunk permit vlan 501 to 503
```

   # Configure the port as a DHCP snooping trusted and ARP trusted port.

```
[SwitchC-Ten-GigabitEthernet1/0/3] dhcp snooping trust
[SwitchC-Ten-GigabitEthernet1/0/3] arp detection trust
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

Configuring Switch D

Create the translated VLANs.

```
<SwitchD> system-view
[SwitchD] vlan 501 to 503
```

Configure Ten-GigabitEthernet 1/0/1 as a trunk port. Assign the port to the translated VLANs 501 through 503.

```
[SwitchD] interface ten-gigabitethernet 1/0/1
[SwitchD-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-Ten-GigabitEthernet1/0/1] port trunk permit vlan 501 to 503
[SwitchD-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify the VLAN mappings on the wiring-closet switches. This example uses Switch A.

```
[SwitchA] display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
```

```
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           101                      N/A
  2             N/A           201                      N/A
  3             N/A           301                      N/A
Interface Ten-GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           102                      N/A
  2             N/A           202                      N/A
  3             N/A           302                      N/A
```

Verify the VLAN mappings on Switch C.

```
[SwitchC] display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  101-102       N/A           501                      N/A
  201-202       N/A           502                      N/A
  301-302       N/A           503                      N/A
Interface Ten-GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  103-104       N/A           501                      N/A
  203-204       N/A           502                      N/A
  303-304       N/A           503                      N/A
```

Configuration files

- Switch A:

```
#
vlan 1
#
vlan 2 to 3
#
vlan 101 to 102
#
vlan 201 to 202
#
vlan 301 to 302
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 3 101 201 301
 vlan mapping 1 translated-vlan 101
 vlan mapping 2 translated-vlan 201
 vlan mapping 3 translated-vlan 301
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 3 102 202 302
 vlan mapping 1 translated-vlan 102
 vlan mapping 2 translated-vlan 202
```

```
 vlan mapping 3 translated-vlan 302
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 101 to 102 201 to 202 301 to 302
#
```

- Switch B:

```
#
vlan 1
#
vlan 2 to 3
#
vlan 103 to 104
#
vlan 203 to 204
#
vlan 303 to 304
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 3 103 203 303
 vlan mapping 1 translated-vlan 103
 vlan mapping 2 translated-vlan 203
 vlan mapping 3 translated-vlan 303
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 3 104 204 304
 vlan mapping 1 translated-vlan 104
 vlan mapping 2 translated-vlan 204
 vlan mapping 3 translated-vlan 304
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 103 to 104 203 to 204 303 to 304
#
```

- Switch C:

```
#
 dhcp snooping enable
#
vlan 101
 arp detection enable
#
vlan 102
 arp detection enable
#
vlan 103
 arp detection enable
```

```
#
vlan 104
 arp detection enable
#
vlan 201
 arp detection enable
#
vlan 202
 arp detection enable
#
vlan 203
 arp detection enable
#
vlan 204
 arp detection enable
#
vlan 301
 arp detection enable
#
vlan 302
 arp detection enable
#
vlan 303
 arp detection enable
#
vlan 304
 arp detection enable
#
vlan 501
 arp detection enable
#
vlan 502
 arp detection enable
#
vlan 503
 arp detection enable
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 101 to 102 201 to 202 301 to 302 501 to 503
 vlan mapping uni range 101 to 102 translated-vlan 501
 vlan mapping uni range 201 to 202 translated-vlan 502
 vlan mapping uni range 301 to 302 translated-vlan 503
 dhcp snooping binding record
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 103 to 104 203 to 204 303 to 304 501 to 503
```

```
 vlan mapping uni range 103 to 104 translated-vlan 501
 vlan mapping uni range 203 to 204 translated-vlan 502
 vlan mapping uni range 303 to 304 translated-vlan 503
 dhcp snooping binding record
#
interface Ten-GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 501 to 503
 vlan mapping nni
 arp detection trust
 dhcp snooping trust
#
```

- Switch D:

```
#
vlan 501 to 503
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 501 to 503
```

Example: Configuring two-to-two VLAN mapping

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

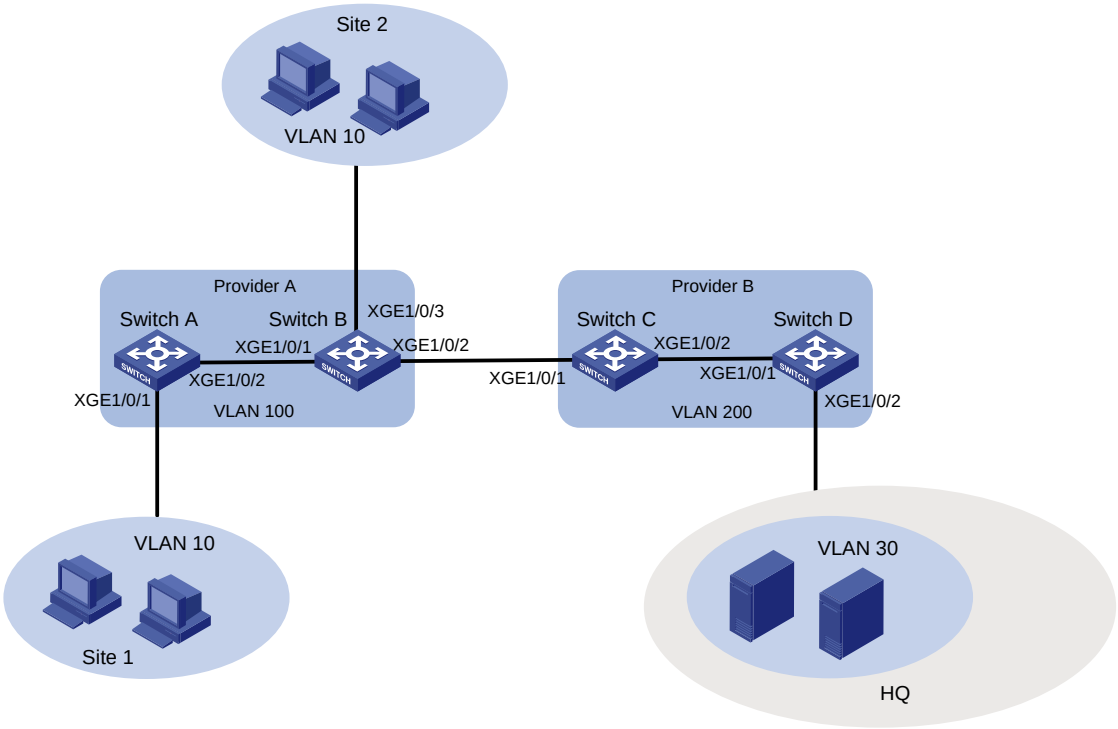
Network requirements

As shown in Figure 249:

- A company assigns its branch sites (Site 1 and Site 2) to VLAN 10, and uses VLAN 30 at the headquarters to provide services for the branch sites.
- Service provider A uses SVLAN 100 to transmit VLAN 10 traffic for the two sites.
- Service provider B uses SVLAN 200 to transmit VLAN 30 traffic for the headquarters.

For the two sites to access VLAN 30 of the headquarters without changing their VLAN assignment, configure two-to-two VLAN mappings on Switch C.

Figure 249 Network diagram



Configuration restrictions and guidelines

You need to configure two-to-two VLAN mappings only on one of the edge devices between the two service provider networks.

Configuration procedures

Configuring Switch A

Create SVLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
```

Configure QinQ on Ten-GigabitEthernet 1/0/1 to add SVLAN tag 100 to traffic from VLAN 10.

```
[SwitchA] interface ten-GigabitEthernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port access vlan 100
[SwitchA-Ten-GigabitEthernet1/0/1] qinq enable
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Configure the network-side port Ten-GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
```

Assign Ten-GigabitEthernet 1/0/2 to VLAN 100.

```
[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Remove Ten-GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchA-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch B

Create SVLAN 100.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit
```

Configure QinQ on Ten-GigabitEthernet 1/0/3 to add SVLAN tag 100 to traffic from VLAN 10.

```
[SwitchB] interface ten-gigabitethernet 1/0/3
[SwitchB-Ten-GigabitEthernet1/0/3] port access vlan 100
[SwitchB-Ten-GigabitEthernet1/0/3] qinq enable
[SwitchB-Ten-GigabitEthernet1/0/3] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a trunk port, assign it to VLAN 100, and remove it from VLAN 1.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
[SwitchB-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a trunk port, assign it to VLAN 100, and remove it from VLAN 1.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100
[SwitchB-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch C

Create SVLANs 100 and 200.

```
<SwitchC> system-view
[SwitchC] vlan 100
[SwitchC-vlan100] quit
[SwitchC] vlan 200
[SwitchC-vlan200] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a trunk port, assign it to VLANs 100 to 200, and remove it from VLAN 1.

```
[SwitchC] interface ten-Ten-GigabitEthernet 1/0/1
[SwitchC-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[SwitchC-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure a two-to-two VLAN mapping on Ten-GigabitEthernet 1/0/1 to map SVLAN 100 and CVLAN 10 to SVLAN 200 and CVLAN 30, respectively.

```
[SwitchC-Ten-GigabitEthernet1/0/1] vlan mapping tunnel 100 10 translated-vlan 200 30
[SwitchC-Ten-GigabitEthernet1/0/1] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a trunk port, assign it to VLAN 200, and remove it from VLAN 1.

```
[SwitchC] interface ten-gigabitethernet 1/0/2
[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 200
[SwitchC-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchC-Ten-GigabitEthernet1/0/2] quit
```

Configuring Switch D

Create SVLAN 200.

```
<SwitchD> system-view
[SwitchD] vlan 200
[SwitchD-vlan200] quit
```

Configure QinQ on Ten-GigabitEthernet 1/0/2 to add SVLAN tag 200 to packets from VLAN 30.

```
[SwitchD] interface ten-gigabitethernet 1/0/2
[SwitchD-Ten-GigabitEthernet1/0/2] port access vlan 200
[SwitchD-Ten-GigabitEthernet1/0/2] qinq enable
[SwitchD-Ten-GigabitEthernet1/0/2] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a trunk port, assign it to VLAN 200, and remove it from VLAN 1.

```
[SwitchD] interface ten-gigabitethernet 1/0/1
[SwitchD-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-Ten-GigabitEthernet1/0/1] port trunk permit vlan 200
[SwitchD-Ten-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchD-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify the VLAN mapping on Switch C.

```
<SwitchC> display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  100           10            200                      30
```

Configuration files

- Switch A:

```
#
vlan 100
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 100
 qinq enable
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
```

- Switch B:

```
#
vlan 100
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 qinq enable
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 100
 qinq enable
```

- Switch C:

```
#
vlan 100
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 vlan mapping tunnel 100 10 translated-vlan 200 30
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
#
```

- Switch D:

```
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 200
 qinq enable
#
```

Example: Modifying the CVLAN ID through QoS re-marking

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

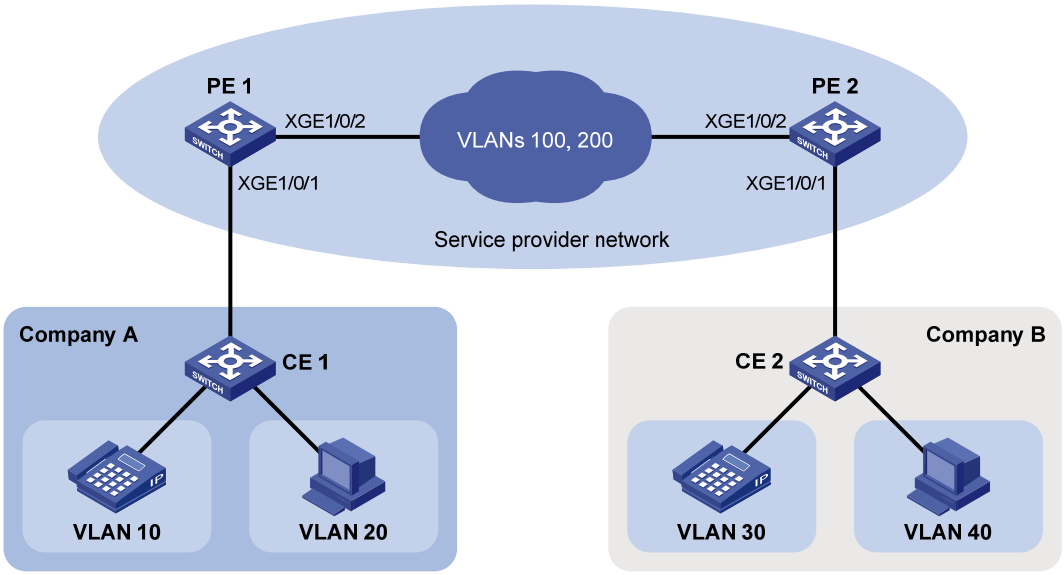
Network requirements

As shown in Figure 250:

- Company A uses CVLANs 10 and 20 to transmit voice traffic and data traffic, respectively.
- Company B uses CVLANs 30 and 40 to transmit voice traffic and data traffic, respectively.
- The service provider uses SVLANs 100 and 200 to transmit these two companies' voice and data traffic, respectively.

To provide Layer 2 connectivity for the voice and data traffic between the two companies, configure one-to-two VLAN mappings and QoS CVLAN re-marking on PE1 and PE 2.

Figure 250 Network diagram



Requirements analysis

To add different SVLAN tags to voice and data traffic, configure one-to-two VLAN mappings on the customer-side ports of PE 1 and PE 2.

To provide Layer 2 connectivity for the traffic from different CVLANs, configure QoS CVLAN re-marking on the service provider-side ports of PE 1 and PE 2.

Configuration procedure

Configuring PE 1

1. Create the CVLANs and SVLANs.

```
<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
[PE1] vlan 30
[PE1-vlan30] quit
[PE1] vlan 40
[PE1-vlan40] quit
```

2. Configure the customer-side port GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port.

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
```

   # Assign the port to VLANs 10 and 20 as a tagged VLAN member.

```
[PE1-GigabitEthernet1/0/1] port hybrid vlan 10 20 tagged
```

   # Assign the port to VLANs 100 and 200 as an untagged VLAN member.

```
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

   # Remove the port from VLAN 1.

```
[PE1-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Configure a one-to-two VLAN mapping to add SVLAN tag 100 to traffic from VLAN 10.

```
[PE1-GigabitEthernet1/0/1] vlan mapping nest single 10 nested-vlan 100
```

   # Configure a one-to-two VLAN mapping to add SVLAN tag 200 to traffic from VLAN 20.

```
[PE1-GigabitEthernet1/0/1] vlan mapping nest single 20 nested-vlan 200
[PE1-GigabitEthernet1/0/1] quit
```

3. Configure the service provider-side port GigabitEthernet 1/0/2:

   # Configure the port as a trunk port.

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

   # Assign the port to VLANs 100 and 200, and remove the port from VLAN 1.

```
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[PE1-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE1-GigabitEthernet1/0/2] quit
```

   # Create the class **A100** to match frames with CVLAN 10 and SVLAN 100.

```
[PE1] traffic classifier A100
[PE1-classifier-A100] if-match customer-vlan-id 10
[PE1-classifier-A100] if-match service-vlan-id 100
[PE1-classifier-A100] quit
```

Configure the traffic behavior **T100** to re-mark matching traffic with CVLAN 30.

```
[PE1] traffic behavior T100
[PE1-behavior-T100] remark customer-vlan-id 30
[PE1-behavior-T100] quit
```

Create the class **A200** to match frames with CVLAN 20 and SVLAN 200.

```
[PE1] traffic classifier A200
[PE1-classifier-A200] if-match customer-vlan-id 20
[PE1-classifier-A200] if-match service-vlan-id 200
[PE1-classifier-A200] quit
```

Configure the traffic behavior **T200** to re-mark matching traffic with CVLAN 40.

```
[PE1] traffic behavior T200
[PE1-behavior-T200] remark customer-vlan-id 40
[PE1-behavior-T200] quit
```

Create the QoS policy **vlanmapping**. In the policy, associate the traffic class **A100** with the traffic behavior **T100**, and associate the traffic class **A200** with the traffic behavior **T200**.

```
[PE1] qos policy vlanmapping
[PE1-qospolicy-vlanmapping] classifier A100 behavior T100
[PE1-qospolicy-vlanmapping] classifier A200 behavior T200
[PE1-qospolicy-vlanmapping] quit
```

Apply the QoS policy to the outgoing traffic on the port.

```
[PE1-GigabitEthernet1/0/2] qos apply policy vlanmapping outbound
[PE1-GigabitEthernet1/0/2] quit
```

Configuring PE 2

1. Create the CVLANs and SVLANs.

```
<PE2> system-view
[PE2] vlan 30
[PE2-vlan30] quit
[PE2] vlan 40
[PE2-vlan40] quit
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] vlan 200
[PE2-vlan200] quit
[PE2] vlan 10
[PE2-vlan10] quit
[PE2] vlan 20
[PE2-vlan20] quit
```

2. Configure the customer-side port GigabitEthernet 1/0/1:

Configure the port as a hybrid port.

```
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type hybrid
```

Assign the port to VLANs 30 and 40 as a tagged VLAN member.

```
[PE2-GigabitEthernet1/0/1] port hybrid vlan 30 40 tagged
```

Assign the port to VLANs 100 and 200 as an untagged VLAN member.

```
[PE2-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Remove the port from VLAN 1.

```
[PE2-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Configure a one-to-two VLAN mapping to add SVLAN tag 100 to traffic from VLAN 30.

```
[PE2-GigabitEthernet1/0/1] vlan mapping nest single 30 nested-vlan 100
```

Configure a one-to-two VLAN mapping to add SVLAN tag 200 to traffic from VLAN 40.

```
[PE2-GigabitEthernet1/0/1] vlan mapping nest single 40 nested-vlan 200
[PE2-GigabitEthernet1/0/1] quit
```

3. Configure the service provider-side port GigabitEthernet 1/0/2:

Configure the port as a trunk port.

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLANs 100 and 200.

```
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Remove the port from VLAN 1.

```
[PE2-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE2-GigabitEthernet1/0/2] quit
```

Create the class **A100** to match frames with CVLAN 30 and SVLAN 100.

```
[PE2] traffic classifier A100
[PE2-classifier-A100] if-match customer-vlan-id 30
[PE2-classifier-A100] if-match service-vlan-id 100
[PE2-classifier-A100] quit
```

Configure the traffic behavior **T100** to re-mark matching traffic with CVLAN 10.

```
[PE2] traffic behavior T100
[PE2-behavior-T100] remark customer-vlan-id 10
[PE2-behavior-T100] quit
```

Create the class **A200** to match frames with CVLAN 40 and SVLAN 200.

```
[PE2] traffic classifier A200
[PE2-classifier-A200] if-match customer-vlan-id 40
[PE2-classifier-A200] if-match service-vlan-id 200
[PE2-classifier-A200] quit
```

Configure the traffic behavior **T200** to re-mark matching packets with CVLAN 20.

```
[PE2] traffic behavior T200
[PE2-behavior-T200] remark customer-vlan-id 20
[PE2-behavior-T200] quit
```

Create the QoS policy **vlanmapping**. In the policy, associate the traffic class **A100** with the traffic behavior **T100**, and associate the traffic class **A200** with the traffic behavior **T200**.

```
[PE2] qos policy vlanmapping
[PE2-qospolicy-vlanmapping] classifier A100 behavior T100
[PE2-qospolicy-vlanmapping] classifier A200 behavior T200
[PE2-qospolicy-vlanmapping] quit
```

Apply the QoS policy to the outgoing traffic on the port.

```
[PE2] interface gigabitethernet 1/0/2
```

```
[PE1-GigabitEthernet1/0/2] qos apply policy vlanmapping outbound
[PE2-GigabitEthernet1/0/2] quit
```

Configuring third-party devices

Configure the ports between PE 1 and PE 2 to allow frames from VLANs 100 and 200 to pass through tagged. (Details not shown.)

Verifying the configuration

Verify the VLAN mappings on the service provider edge devices. This example uses PE 1.

```
<PE 1>display vlan mapping
Interface Ten-GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10            N/A           100                      10
  20            N/A           200                      20
```

Verify the QoS policy configuration. This example uses Ten-GigabitEthernet 1/0/2 of PE 1.

```
<PE 1> display qos policy interface Ten-GigabitEthernet 1/0/2

Interface: Ten-GigabitEthernet1/0/2

  Direction: Outbound

  Policy: vlanmapping
   Classifier: A100
     Operator: AND
     Rule(s) : If-match customer-vlan-id 10
               If-match service-vlan-id 100
     Behavior: T100
      Marking:
        Remark Customer VLAN ID 30
   Classifier: A200
     Operator: AND
     Rule(s) : If-match customer-vlan-id 20
               If-match service-vlan-id 200
     Behavior: T200
      Marking:
        Remark Customer VLAN ID 40
```

Configuration files

- PE 1:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
```

```
vlan 40
#
vlan 100
#
vlan 200
#
traffic classifier A100 operator and
 if-match customer-vlan-id 10
 if-match service-vlan-id 100
#
traffic classifier A200 operator and
 if-match customer-vlan-id 20
 if-match service-vlan-id 200
#
traffic behavior T100
 remark customer-vlan-id 30
#
traffic behavior T200
 remark customer-vlan-id 40
#
qos policy vlanmapping
 classifier A100 behavior T100
 classifier A200 behavior T200
#
interface Ten-GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 20 tagged
 port hybrid vlan 100 200 untagged
 vlan mapping nest single 10 nested-vlan 100
 vlan mapping nest single 20 nested-vlan 200
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 qos apply policy vlanmapping outbound
#
```

- PE 2:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
```

```
vlan 100
#
vlan 200
#
traffic classifier A100 operator and
 if-match customer-vlan-id 30
 if-match service-vlan-id 100
#
traffic classifier A200 operator and
 if-match customer-vlan-id 40
 if-match service-vlan-id 200
#
traffic behavior T100
 remark customer-vlan-id 10
#
traffic behavior T200
 remark customer-vlan-id 20
#
qos policy vlanmapping
 classifier A100 behavior T100
 classifier A200 behavior T200
#
interface Ten-GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 20 tagged
 port hybrid vlan 100 200 untagged
 vlan mapping nest single 30 nested-vlan 100
 vlan mapping nest single 40 nested-vlan 200
#
interface Ten-GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 qos apply policy vlanmapping outbound
#
```

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 being tagged. This value might differ by vendor. In a multi-vendor network, you must set the TPID setting on one vendor's device to be compatible with another vendor's device for 802.1Q tagged frames to be identified correctly.

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

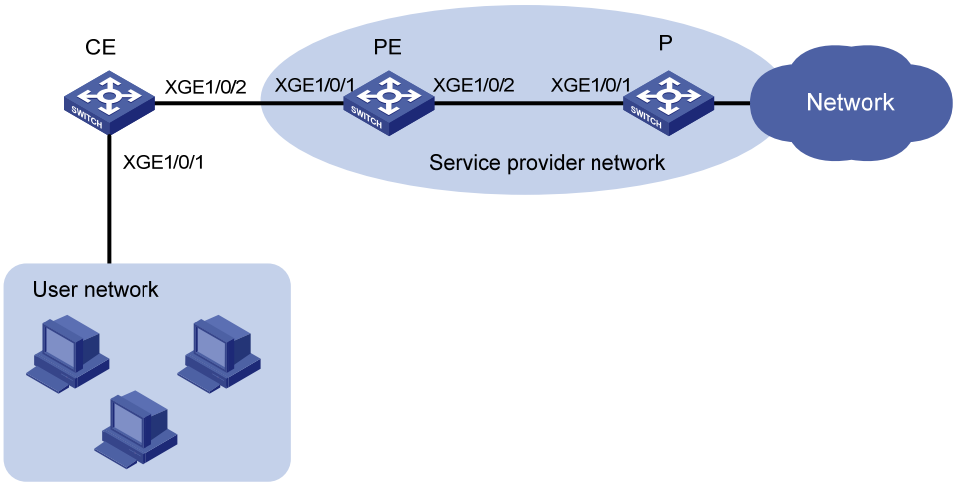
Network requirements

As shown in Figure 251:

- QinQ is enabled on Ten-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 251 Network diagram



Requirements analysis

The switch supports one global CVLAN PVID for all QinQ-enabled ports. On a QinQ-enabled port, 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 SVLAN tagging QoS policies or VLAN mapping, you must make sure The CVLAN TPID on the switch is the same as the VLAN TPID on the customer device. TPID mismatch can result in SVLAN assignment mistake. If you are implementing 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 Ten-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 Ten-GigabitEthernet 1/0/2 of the PE.

Configuration restrictions and guidelines

Configure the SVLAN TPID on the service provider-side ports. You cannot configure the SVLAN TPID on QinQ-enabled ports.

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 the customer-side port Ten-GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port, set its PVID to 1000, and remove it from VLAN 1.

```
[PE] interface ten-gigabitethernet 1/0/1
[PE-Ten-GigabitEthernet1/0/1] port link-type hybrid
[PE-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 1000
[PE-Ten-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Assign the port to VLAN 1000 as an untagged VLAN member.

```
[PE-Ten-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

   # Enable QinQ on the port.

```
[PE-Ten-GigabitEthernet1/0/1] qinq enable
[PE-Ten-GigabitEthernet1/0/1] quit
```

4. Configure the service-provider-side port Ten-GigabitEthernet 1/0/2:

   # Configure the port as a trunk port, assign it to VLAN 1000, and remove it from VLAN 1.

```
[PE] interface ten-gigabitethernet 1/0/2
[PE-Ten-GigabitEthernet1/0/2] port link-type trunk
[PE-Ten-GigabitEthernet1/0/2] port trunk permit vlan 1000
[PE-Ten-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

   # Set the SVLAN TPID to 0x9100 on the port.

```
[PE-Ten-GigabitEthernet1/0/2] qinq ethernet-type service-tag 9100
[PE-Ten-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 ten-gigabitethernet 1/0/2
```

```
[PE-Ten-GigabitEthernet1/0/2] display this
#
interface ten-gigabitethernet1/0/2
 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 ten-gigabitethernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
interface ten-gigabitethernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000
 qinq ethernet-type service-tag 9100
#
```

IPv4-based VRRP configuration examples

This chapter provides IPv4-based VRRP configuration examples, including load-balanced VRRP and using VRRP with the Track module.

For a quick master/backup switchover when the uplink on the master fails, you can configure a track entry to monitor the master's uplink state. The monitoring protocols available for the track entry include NQA, interface management, and BFD.

Example: Configuring a single VRRP group

Applicable product matrix

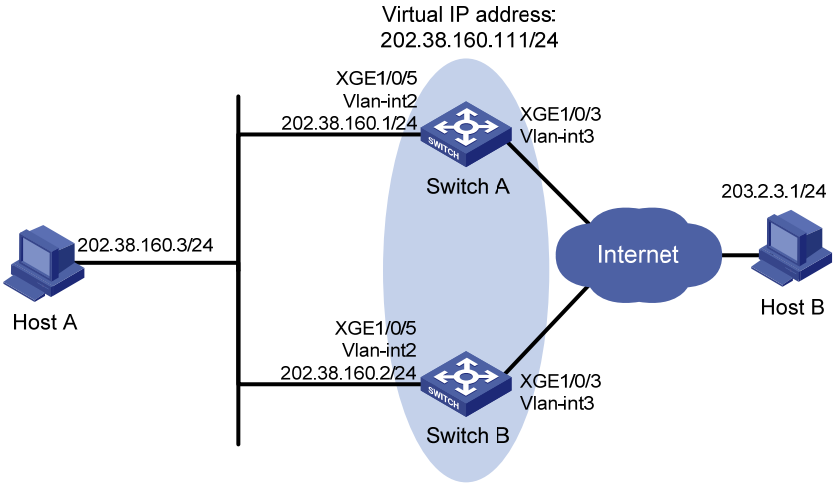
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 252, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet 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.

Figure 252 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.

To enable the switches in the VRRP group to process only 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 Switch A:

   # Configure VLAN 3.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 3
   [SwitchA-vlan3] port ten-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 ten-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
   ```

   # Specify VRRPv2 to run on interface VLAN-interface 2.

   ```
   [SwitchA-Vlan-interface2] vrrp version 2
   ```

   # 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 plain 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 delay 5
   ```

2. Configure Switch B:

   # Configure VLAN 3.

   ```
   <SwitchB> system-view
   [SwitchB] vlan 3
   [SwitchB-vlan3] port ten-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] vlan 2
[SwitchB-Vlan2] port ten-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
```

Specify VRRPv2 to run on interface VLAN-interface 2.

```
[SwitchA-Vlan-interface2] vrrp version 2
[SwitchB-Vlan-interface2] vrrp version 2
```

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 plain 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 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 Virtual Router Information:
 Running Mode      : Standard
 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     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 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
```

```
    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 Virtual Router Information:
 Running Mode      : Standard
 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      : 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.

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 version 2
 vrrp vrid 1 authentication-mode simple cipher $c$3$8FYX05mfiOPG4CdvYwH3SGBrLEK2
jV7u
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5
#
interface Vlan-interface3
 ip address 100.0.0.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-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 version 2
 vrrp vrid 1 authentication-mode simple cipher $c$3$KLtbH0Gbizn+zRMFWR/quLufRq6D
uDBT
 vrrp vrid 1 preempt-mode delay 5
#
interface Vlan-interface3
 ip address 101.0.0.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring a track entry to monitor the uplink on the master by using interface management

Applicable product matrix

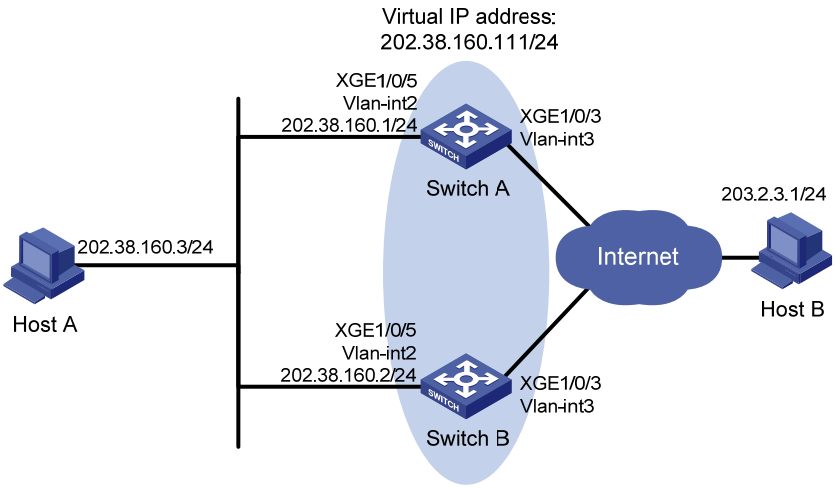
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 253, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet the following requirements:

- Switch A operates as the master. When Switch A or its uplink interface fails, Switch B takes over to forward packets for the hosts.
- Create a track entry to monitor the uplink state on Switch A by using the interface management module. When the uplink fails, the priority of Switch A decreases, and Switch B takes over quickly to forward traffic.

Figure 253 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.

Configuration restrictions and guidelines

When you configure a single 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 the value by which the priority of a switch decreases, make sure the decreased priority of the switch is lower than the priority of all the other switches in the VRRP group. This makes ensure a switch in the group can be elected as the master.

Configuration procedures

1. Configure VLANs and IP addresses for VLAN interfaces on Switch A and Switch B:

   # On Switch A, Configure VLAN 3 and the IP address for VLAN-interface 3.

```
<SwitchA> system-view
[SwitchA] vlan 3
[SwitchA-vlan3] port ten-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
```

   # On Switch A, Configure VLAN 2 and the IP address for VLAN-interface 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port ten-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
```

On Switch B, Configure VLAN 3 and the IP address for VLAN-interface 3.

```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-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
```

On Switch B, Configure VLAN 2 and the IP address for VLAN-interface 2.

```
[SwitchB] vlan 2
[SwitchB-Vlan2] port ten-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
```

2. Configure a track entry and VRRP on Switch A:

   # Configure track entry 1 to monitor the link status of the uplink interface VLAN-interface 3 by using the interface management module.

   ```
   [SwitchA] track 1 interface vlan-interface 3
   ```

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 202.38.160.111/24.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
   ```

   # Set the priority of Switch A in VRRP group 1 to 110.

   ```
   [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 delay 5
   ```

   # Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch 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
   ```

3. Configure VRRP on Switch B:

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 202.38.160.111/24.

   ```
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
   ```

   # Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5
   ```

4. 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 to verify that the two hosts are reachable to each other. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
```

```
IPv4 Virtual Router Information:
 Running Mode      : Standard
 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      : None
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
   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 Virtual Router Information:
 Running Mode      : Standard
 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
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.1
```

The output shows that in VRRP group 1, Switch A is the master, and Switch B is a backup. Packets from Host A to Host B are forwarded through Switch A.

When Switch A fails, 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 Virtual Router Information:
 Running Mode      : Standard
 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      : None
     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 becomes the master. Packets from Host A to Host B are forwarded through Switch B.

When VLAN-interface 3 on Switch A fails, you can still successfully ping Host B on Host A.

Display detailed information about VRRP group 1 on Switch A.

```
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 100
     Admin Status   : Up                State         : Backup
     Config Pri     : 110               Running Pri   : 90
     Preempt Mode   : Yes               Delay Time    : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.2
   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 Virtual Router Information:
 Running Mode      : Standard
 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      : None
     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 to 90. Switch A becomes the backup, and Switch B becomes the master. Packets from Host A to Host B are forwarded through Switch B.

Configuration files

- 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 delay 5
 vrrp vrid 1 track 1 reduced 20
#
interface Vlan-interface3
 ip address 100.0.0.2 255.255.255.0
```

```
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
 track 1 interface Vlan-interface3
#
```

- 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 delay 5
#
interface Vlan-interface3
 ip address 101.0.0.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring a track entry to monitor the uplink on the master by using NQA

Applicable product matrix

Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

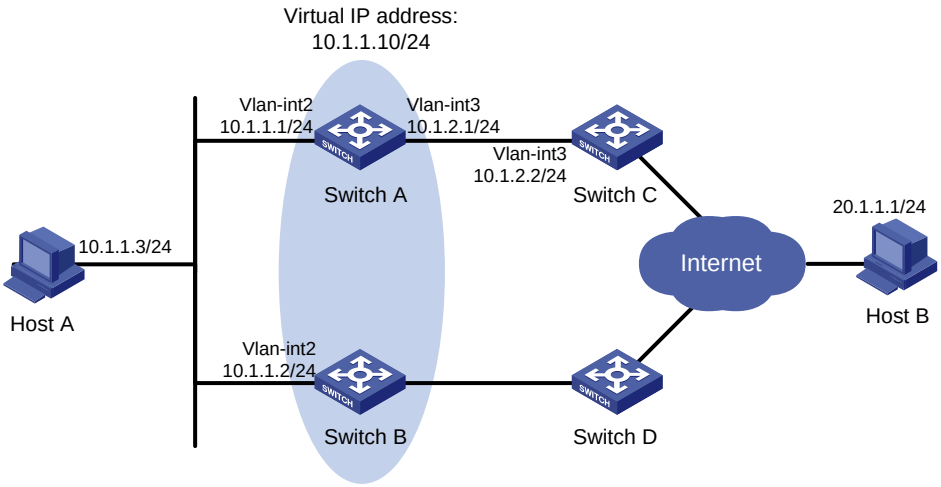
Network requirements

As shown in Figure 254, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet the following requirements:

- Switch A operates as the master. When Switch A fails, Switch B takes over to forward packets for the hosts.

- Create a track entry to monitor the uplink state on Switch A by using NQA. When the uplink fails, the priority of Switch A decreases, and Switch B takes over quickly to forward traffic.

Figure 254 Network diagram



Requirements analysis

To enable 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.

To enable the switches in the VRRP group to process only 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 254. This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way.

   # Specify an IP address for VLAN-interface 2 on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port ten-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**. Start the operation.

```
[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:

Specify VRRPv2 to run on interface VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp version 2
```

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.10.

```
[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 plain 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 delay 5
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch 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:

Specify VRRPv2 to run on interface VLAN-interface 2.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp version 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 plain 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 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 Virtual Router Information:
 Running Mode      : Standard
 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     : 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 Virtual Router Information:
 Running Mode      : Standard
 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
     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.

When Switch A fails, 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 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer   : 100
     Admin Status   : Up                State         : Backup
     Config Pri     : 110               Running Pri   : 90
```

```
    Preempt Mode   : Yes                Delay Time   : 5
    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 Virtual Router Information:
 Running Mode      : Standard
 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     : 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
#
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
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 vrrp version 2
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 authentication-mode simple cipher $c$3$5V4aEt1GW0E63mhGOEtGgPn15cD2
+6Pg
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 reduced 20
```

```
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
interface Ten-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
#
 nqa schedule admin test start-time now lifetime forever
#
 track 1 nqa entry admin test reaction 1
#
```

- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp version 2
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 authentication-mode simple cipher $c$3$eF9q3pB/ILjMRBdGv2mF9sHkfSFw
EqZC
 vrrp vrid 1 preempt-mode delay 5
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring a track entry to monitor the uplink on the master by using BFD

Applicable product matrix

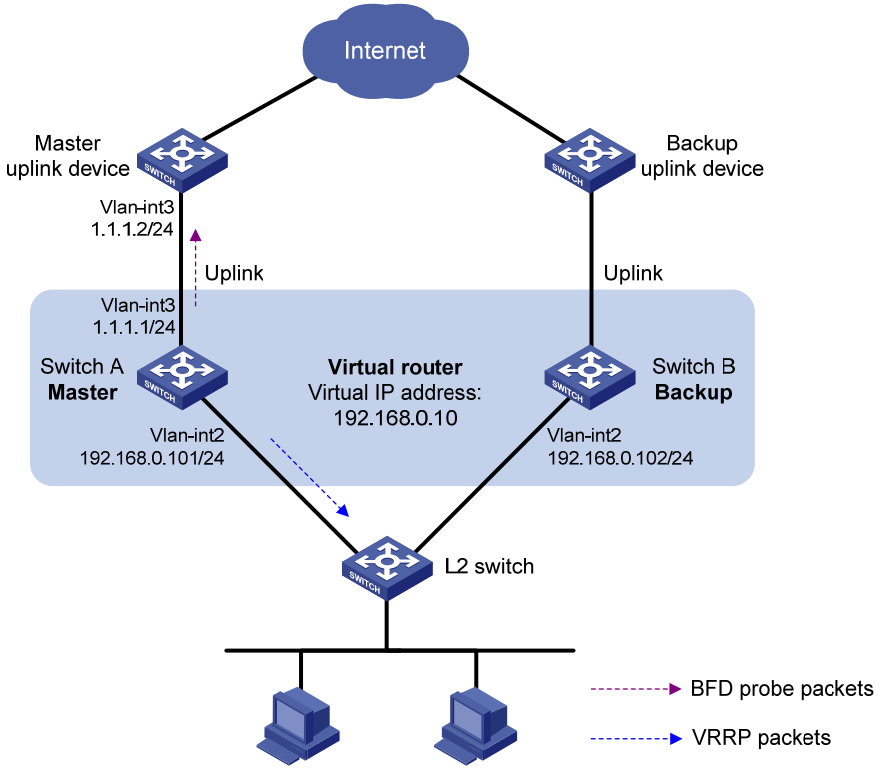
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 255, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet the following requirements:

- Switch A operates as the master. When Switch A fails, Switch B takes over to forward packets for the hosts.
- Create a track entry to monitor the uplink state on Switch A by using BFD. When the uplink fails, the priority of Switch A decreases, and Switch B takes over quickly to forward traffic.

Figure 255 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.

To enable the switches in the VRRP group to process only 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 them 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 255. This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way.

   # Specify an IP address for VLAN-interface 2 on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port ten-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:

   # Create track entry 1 to monitor the link between local IP address 1.1.1.1 and remote IP address 1.1.1.2 by sending BFD echo packets.

   ```
   [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:

   # Specify VRRPv2 to run on interface VLAN-interface 2.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp version 2
   ```

   # 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 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 plain hello
   ```

   # Associate VRRP group 1 on VLAN-interface 2 with track entry 1. 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:

   # Specify VRRPv2 to run on interface VLAN-interface 2.

   ```
   <SwitchB> system-view
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp version 2
   ```

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 192.168.0.10.

```
[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 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 plain 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 Virtual Router Information:
 Running Mode      : Standard
 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     : 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
  State: Positive
  Duration: 0 days 0 hours 2 minutes 31 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface3
    VPN instance name: -
    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 Virtual Router Information:
 Running Mode      : Standard
 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
    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 the backup.

When the uplink of Switch A goes down, display detailed information about track entry 1 on Switch A.

```
<SwitchA> display track 1
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 2 minutes 23 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface3
    VPN instance name: -
    Remote IP: 1.1.1.2
    Local IP: 1.1.1.1
```

The output shows that the status of track entry 1 becomes **Negative**.

Display detailed information about VRRP group 1 on Switch A.

```
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 110                Running Pri  : 90
     Preempt Mode   : Yes                Delay Time   : 5
     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 Virtual Router Information:
 Running Mode      : Standard
 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     : 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 version 2
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 authentication-mode simple cipher $c$3$HglsaiHZm13Y3LMDDUTETCmrR4qa
QyV1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 reduced 20
#
interface Vlan-interface3
 ip address 1.1.1.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
interface Ten-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 version 2
 vrrp vrid 1 virtual-ip 192.168.0.10
```

```
 vrrp vrid 1 authentication-mode simple cipher $c$3$k0xj3ouPzhX0CT80tmHrJRYVLKyC
jEO/
 vrrp vrid 1 preempt-mode delay 5
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring a track entry to monitor the master on a backup by using BFD

Applicable product matrix

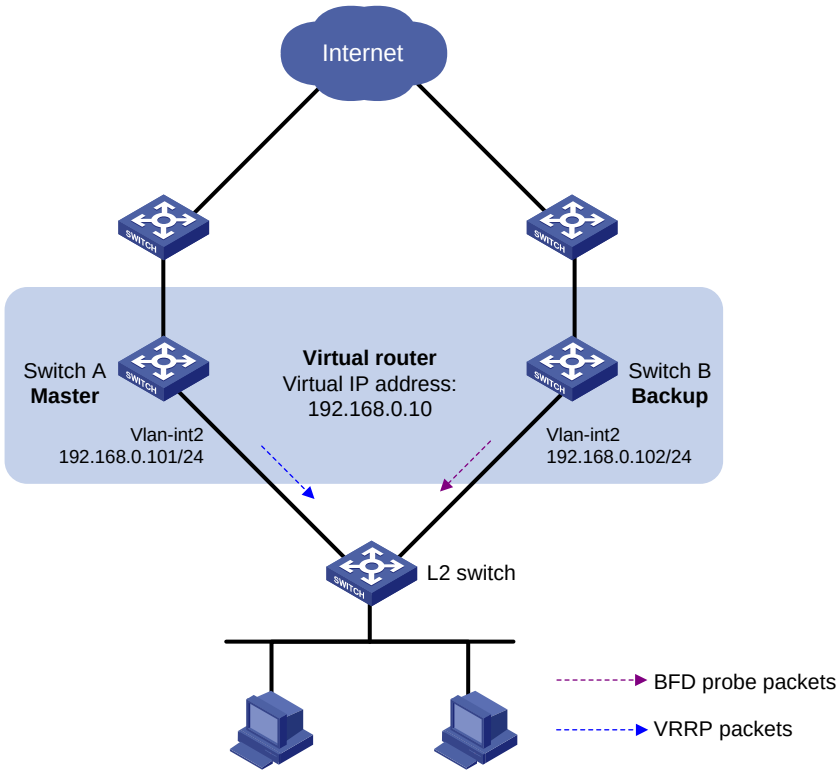
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 256, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet the following requirements:

- Switch A operates as the master. When Switch A fails, Switch B takes over to forward packets for the hosts.
- Create a track entry to monitor the uplink state on Switch A by using BFD. When the uplink fails, the priority of Switch A decreases, and Switch B takes over quickly to forward traffic.

Figure 256 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.

To enable the switches in the VRRP group to process only 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 them 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 256. This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way.

   # Configure Switch A:

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   ```

```
[SwitchA-vlan2] port ten-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:

   # Specify VRRPv2 to run on interface VLAN-interface 2.

   ```
   [SwitchA-Vlan-interface2] vrrp version 2
   ```

   # 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 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 plain 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 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:

   # Specify VRRPv2 to run on interface VLAN-interface 2.

   ```
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp version 2
   ```

   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

   ```
   [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 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 plain 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 Virtual Router Information:
 Running Mode      : Standard
 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     : 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 Virtual Router Information:
 Running Mode      : Standard
 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
     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 5 minutes 28 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: -
    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 the backup.

Enable VRRP state debugging and BFD event debugging on Switch B.

```
<SwitchB> terminal debugging
```

```
<SwitchB> terminal monitor
<SwitchB> debugging vrrp fsm
<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 Virtual Router Information:
 Running Mode      : Standard
 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     : 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, it notifies VRRP through the Track module to change the status of Switch B to master without waiting for a period three times the advertisement interval. This makes sure a backup can quickly 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:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.101 255.255.255.0
 vrrp version 2
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 authentication-mode simple cipher $c$3$6J/P5VU4+S+yNIKIzGhVr6KX8NHT
DJMz
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

- Switch B:

```
#
 bfd echo-source-ip 10.10.10.10
#
vlan 2
#
interface Vlan-interface2
interface Vlan-interface2
 vrrp version 2
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 authentication-mode simple cipher $c$3$YSfP4gcRp1I/+z0a5i02UBb8IyW7
E9SU
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 switchover
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
track 1 bfd echo interface vlan-interface2 remote ip 192.168.0.101 local ip
192.168.0.102
#
```

Example: Configuring multiple VRRP groups for load balancing

Applicable product matrix

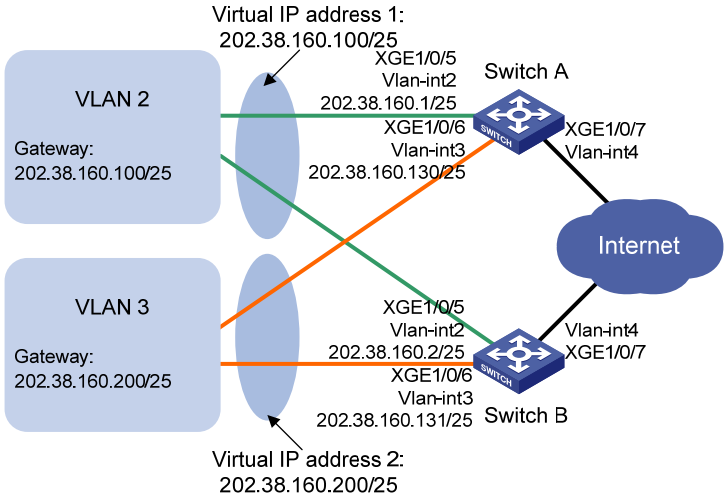
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 257, configure two VRRP groups on Switch A and Switch B to meet the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2. 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.
- Create a track entry to monitor the uplink state on the switches by using the interface management module. When the uplink fails, the priority of the corresponding switch decreases, and the other switch takes over quickly to forward traffic.

Figure 257 Network diagram



- You can configure collaboration between VRRP and Track, NQA, or BFD on the master to monitor the uplink status. For more information, see "Example: Configuring a track entry to monitor the uplink on the master by using NQA."
- You can configure BFD for a VRRP backup to monitor the master. For more information, see "Example: Configuring a track entry to monitor the master on a backup by using BFD."

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.

Configuration restrictions and guidelines

When you configure multiple VRRP groups, follow these 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 them is also the same.
- When you configure the value by which the priority of a switch decreases, make sure the decreased priority of the switch is lower than the priority of all the other switches in the VRRP group. This makes ensure a switch in the group can be elected as the master.

Configuration procedures

1. Configure Switch A:

   # Configure VLAN 4.

```
<SwitchA> system-view
[SwitchA] vlan 4
[SwitchA-vlan4] port ten-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 track entry 1 to monitor the link status of the uplink interface VLAN-interface 4 by using the interface management module.

```
[SwitchA] track 1 interface vlan-interface 4
```

Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port ten-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 delay 5
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 30 when the state of track entry 1 changes to negative.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 30
[SwitchA-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port ten-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 delay 5
```

2. Configure Switch B:

Configure VLAN 4.

```
<SwitchB> system-view
[SwitchB] vlan 4
[SwitchB-vlan4] port ten-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 track entry 1 to monitor the link status of the uplink interface VLAN-interface 4 by using the interface management module.

```
[SwitchB] track 1 interface vlan-interface 4
```

Configure VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port ten-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 delay 5
[SwitchB-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-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 delay 5
```

Associate VRRP group 1 on VLAN-interface 3 with track entry 1. Decrease the priority of the switch in the VRRP group by 30 when the state of track entry 1 changes to negative.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 track 1 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 Virtual Router Information:
 Running Mode      : Standard
 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     : 202.38.160.100
     Virtual MAC    : 0000-5e00-011e
     Master IP      : 202.38.160.1
   VRRP Track Information:
     Track Object   : 1                 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
    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 Virtual Router Information:
 Running Mode      : Standard
 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
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Master IP      : 202.38.160.1

   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     : 202.38.160.200
     Virtual MAC    : 0000-5e00-0120
     Master IP      : 202.38.160.131
   VRRP Track Information:
     Track Object   : 1                  State : Up         Pri Reduced : 30
```

The output shows that:

- 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 groups on Switch B when Switch A fails.

```
[SwitchB-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 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     : 202.38.160.100
```

```
    Virtual MAC    : 0000-5e00-011e
    Master IP      : 202.38.160.2

  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     : 202.38.160.200
    Virtual MAC    : 0000-5e00-0120
    Master IP      : 202.38.160.131
  VRRP Track Information:
    Track Object   : 1                 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.

When VLAN-interface 4 on Switch A fails, hosts in VLAN 2 can still access the external network.

Display detailed information about the VRRP groups on Switch A.

```
IPv4 Virtual Router Information:
 Running Mode      : Standard
 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
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.2
   VRRP Track Information:
     Track Object   : 1                 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
     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.

```
IPv4 Virtual Router Information:
 Running Mode      : Standard
 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     : 202.38.160.100
  Virtual MAC    : 0000-5e00-011e
  Master IP      : 202.38.160.2

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     : 202.38.160.200
  Virtual MAC    : 0000-5e00-0120
  Master IP      : 202.38.160.131
VRRP Track Information:
  Track Object   : 1                  State : Up         Pri Reduced : 30
```

The output shows that when VLAN-interface 4 on Switch A fails, the priority of Switch A decreases to 80. Switch A becomes the backup, and Switch B becomes the master in VRRP group 1. Internet traffic for hosts in VLAN 2 is forwarded through Switch B.

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 delay 5
 vrrp vrid 1 track 1 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 delay 5
#
interface Vlan-interface4
 ip address 20.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/6
 port access vlan 3
```

```
#
interface Ten-GigabitEthernet1/0/7
 port access vlan 4
#
 track 1 interface Vlan-interface4
#
```

- 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 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 delay 5
 vrrp vrid 2 track 1 reduced 30
#
interface Vlan-interface4
 ip address 30.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/6
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/7
 port access vlan 4
#
 track 1 interface Vlan-interface4
#
```

Example: Using VRRP with MSTP

Applicable product matrix

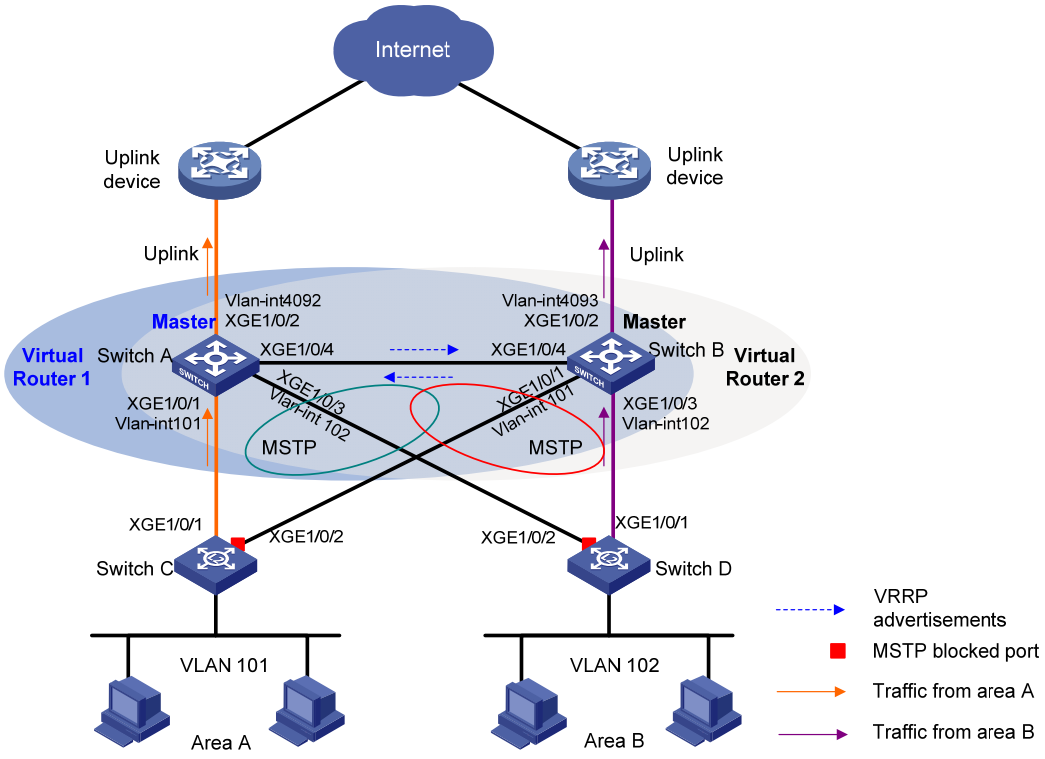
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 258, configure two VRRP groups on Switch A and Switch B to meet the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2. Switch B operates as the master of VRRP group 2 to forward packets from VLAN 3. When one of the switches fails, the other switch provides gateway service for both VLANs.
- Create a track entry to monitor the uplink state on the switches by using the interface management module. When the uplink fails, the priority of the corresponding switch decreases, and the other switch takes over quickly to forward traffic.

Figure 258 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid loops between Switch A, Switch B, Switch C, and Switch D, enable MSTP on them.

Configuration procedures

1. Configure Switch A:

   # Assign Ten-GigabitEthernet 1/0/1 to VLAN 101, Ten-GigabitEthernet 1/0/3 to VLAN 102, and Ten-GigabitEthernet 1/0/2 to VLAN 4092.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 101
   [SwitchA-vlan101] port ten-gigabitethernet 1/0/1
   ```

```
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port ten-gigabitethernet 1/0/3
[SwitchA-vlan102] quit
[SwitchA] vlan 4092
[SwitchA-vlan4092] port ten-gigabitethernet 1/0/2
[SwitchA-vlan4092] quit
```

Configure the link type of Ten-GigabitEthernet 1/0/4 as **trunk**.

```
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/4] undo port trunk permit vlan 1
```

Assign Ten-GigabitEthernet 1/0/4 to VLAN 101 and VLAN 102.

```
[SwitchA-Ten-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchA-Ten-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

Configure the uplink interface.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] undo stp enable
[SwitchA-Ten-GigabitEthernet1/0/2] quit
[SwitchA] interface vlan-interface 4092
[SwitchA-Vlan-interface4092] ip address 10.1.1.2 24
[SwitchA-Vlan-interface4092] quit
```

Configure track entry 1 to monitor the link status of the uplink interface VLAN-interface 4092 by using the interface management module.

```
[SwitchA] track 1 interface vlan-interface 4092
```

Create VRRP group 1, and assign virtual IP address **10.10.101.1** to the VRRP group. Configure the priority of the switch in VRRP group 1 as **110**.

```
[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
```

On VLAN-interface 101, set the interface to be tracked to VLAN-interface 4092. The priority of VRRP group 1 on VLAN-interface 4092 will decrement by 20 when VLAN-interface 101 is down or removed.

```
[SwitchA-Vlan-interface101] vrrp vrid 1 track 1 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 global enable
```

2. Configure Switch B:

Assign Ten-GigabitEthernet 1/0/1 to VLAN 101, Ten-GigabitEthernet 1/0/3 to VLAN 102, and Ten-GigabitEthernet 1/0/2 to VLAN 4093.

```
<SwitchB> system-view
[SwitchB] vlan 101
[SwitchB-vlan101] port ten-gigabitethernet 1/0/1
[SwitchB-vlan101] quit
[SwitchB] vlan 102
[SwitchB-vlan102] port ten-gigabitethernet 1/0/3
[SwitchB-vlan102] quit
[SwitchB] vlan 4093
[SwitchB-vlan4093] port ten-gigabitethernet 1/0/2
[SwitchB-vlan4093] quit
```

Configure the link type of Ten-GigabitEthernet 1/0/4 as trunk.

```
[SwitchB] interface ten-gigabitethernet 1/0/4
[SwitchB-Ten-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/4] undo port trunk permit vlan 1
```

Assign Ten-GigabitEthernet 1/0/4 to VLAN 101 and VLAN 102.

```
[SwitchB-Ten-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchB-Ten-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchB-Ten-GigabitEthernet1/0/4] quit
```

Configure the uplink interface.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] undo stp enable
[SwitchB-Ten-GigabitEthernet1/0/2] quit
[SwitchB] interface vlan-interface 4093
[SwitchB-Vlan-interface4093] ip address 10.1.2.2 24
[SwitchB-Vlan-interface4093] quit
```

Configure track entry 1 to monitor the link status of the uplink interface VLAN-interface 4093 by using the interface management module.

```
[SwitchB] track 1 interface vlan-interface 4093
```

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. Configure the priority of the switch in VRRP group 1 as **110**.

```
[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
```

On VLAN-interface 102, set the interface to be tracked to VLAN-interface 4093. The priority of VRRP group 1 on VLAN-interface 4093 will decrement by 20 when VLAN-interface 102 fails.

```
[SwitchB-Vlan-interface102] vrrp vrid 1 track 1 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 global enable
```

3. Configure Switch C:

Configure VLAN 101.

```
<SwitchC> system-view
[SwitchC] vlan 101
[SwitchC-vlan101] port ten-gigabitethernet 1/0/1 to ten-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 global enable
```

4. Configure Switch D:

Configure VLAN 102.

```
<SwitchD> system-view
[SwitchD] vlan 102
[SwitchD-vlan102] port ten-gigabitethernet 1/0/1 to ten-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 global 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. Execute the **display stp brief** command to display brief information about MSTP. (Details not shown.)

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 global 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 1 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 Ten-GigabitEthernet1/0/1
 port access vlan 101
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 4092
 undo stp enable
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 102
#
interface Ten-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
#
 track 1 interface Vlan-interface4092
#
```

- 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 global 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 1 reduced 20
#
interface Vlan-interface4093
 ip address 10.1.2.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 101
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 4093
 undo stp enable
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 102
#
interface Ten-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
#
 track 1 interface Vlan-interface4093
#
```

- Switch C:

```
#
 vlan 101
#stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp global enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 101
#
interface Ten-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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 102
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 102
#
```

Example: Configuring VRRP load balancing mode

Applicable product matrix

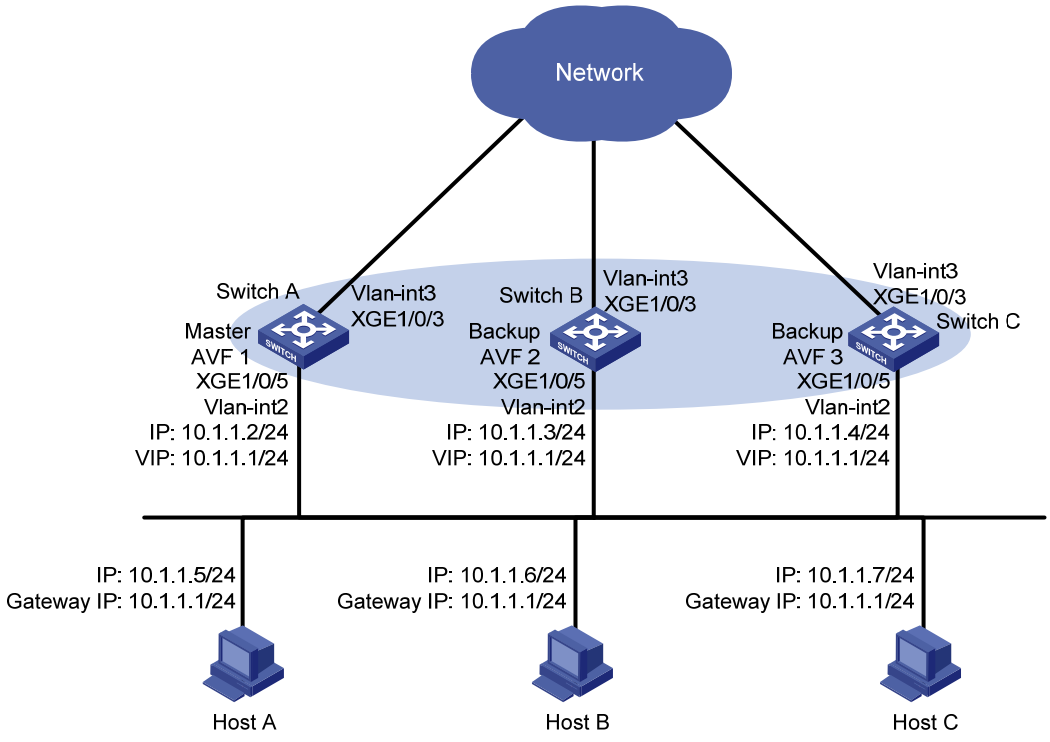
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 259, configure a load-balanced VRRP group on Switch A, Switch B, and Switch C with virtual IP address 10.1.1.1/24 to meet the following requirements:

- Switch A operates as the master to forward packets from Host A. When Switch A fails, Switch B or Switch C takes over to forward packets for Host A.
- Packets from the hosts are forwarded by different switches to reduce the burden of the master.
- Create a track entry to monitor the upstream link of the active virtual forwarder (AVF) by using the interface management module. When the upstream link of the AVF fails, the AVF can notify a listening virtual forwarder (LVF) to take over.

Figure 259 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.

Configuration restrictions and guidelines

When you configure VRRP load balancing mode, follow these restrictions and guidelines:

- In load balancing mode, the virtual IP address of a VRRP group can be any unassigned IP address of the subnet where the VRRP group resides, rather than the IP address of any interface in the VRRP group. No IP address owner can exist in a VRRP group.
- When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255 and does not change with the weight. To guarantee that an LVF can take over the VF owner as the AVF when the upstream link of the VF owner fails, the reduced weight for the VF owner must be higher than 245. This allows the weight of the VF owner to drop below the lower limit of failure.
- 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 Switch A:

   # Configure VLAN 3.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 3
   [SwitchA-vlan3] port ten-gigabitethernet 1/0/3
   [SwitchA-vlan3] quit
   [SwitchA] interface vlan-interface 3
   [SwitchA-Vlan-interface3] ip address 20.1.1.2 24
   [SwitchA-Vlan-interface3] quit
   ```

   # Configure VLAN 2.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] port ten-gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   ```

   # Configure VRRP to operate in load balancing mode.

   ```
   [SwitchA] vrrp mode load-balance
   ```

   # Create VRRP group 1, and set the virtual IP address for the group to **10.1.1.1**.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 10.1.1.2 24
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
   ```

   # Set the priority of Switch A in VRRP group 1 to **120**.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 120
   ```

   # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5
   [SwitchA-Vlan-interface2] quit
   ```

Create track entry 1 to monitor the link state of VLAN-interface 3 by using the interface management module.

```
[SwitchA] track 1 interface vlan-interface 3
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 250 when the state of track entry 1 changes to negative.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

2. Configure Switch B:

Configure VLAN 3.

```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-gigabitethernet 1/0/3
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 30.1.1.2 24
[SwitchB-Vlan-interface3] quit
```

Configure VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port ten-gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchB] vrrp mode load-balance
```

Create VRRP group 1, and set the virtual IP address for the group to **10.1.1.1**.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.3 24
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Set the priority of Switch B in VRRP group 1 to **110**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5
[SwitchB-Vlan-interface2] quit
```

Create track entry 1 to monitor the link state of VLAN-interface 3 by using the interface management module.

```
[SwitchB] track 1 interface vlan-interface 3
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 250 when the state of track entry 1 changes to negative.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

3. Configure Switch C:

Configure VLAN 3.

```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port ten-gigabitethernet 1/0/3
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 40.1.1.2 24
```

```
[SwitchC-Vlan-interface3] quit
```

Configure VLAN 2.

```
[SwitchC] vlan 2
[SwitchC-vlan2] port ten-gigabitethernet 1/0/5
[SwitchC-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchC] vrrp mode load-balance
```

Create VRRP group 1, and set the virtual IP address for the group to **10.1.1.1**.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 10.1.1.4 24
[SwitchC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Configure Switch C to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5
[SwitchC-Vlan-interface2] quit
```

Create track entry 1 to monitor the link state of VLAN-interface 3 by using the interface management module.

```
[SwitchC] track 1 interface vlan-interface 3
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 250 when the state of track entry 1 changes to negative.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

Verifying the configuration

Ping the external network from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                    Adver Timer   : 100
     Admin Status   : Up                   State         : Master
     Config Pri     : 120                  Running Pri   : 120
     Preempt Mode   : Yes                  Delay Time    : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
```

```
    Owner ID       : 0000-5e01-1101
    Priority       : 255
    Active         : local
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : 10.1.1.3
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 110                 Running Pri  : 110
     Preempt Mode   : Yes                 Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.3 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : 10.1.1.2
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
```

```
    State           : Listening
    Virtual MAC     : 000f-e2ff-0013 (Learnt)
    Owner ID        : 0000-5e01-1105
    Priority        : 127
    Active          : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object    : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 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
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : 10.1.1.2
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that in VRRP group 1, Switch A is the master, and Switch B and Switch C are the backups. An active VF and two listening VFs exist on each switch.

Display detailed information about VRRP group 1 on Switch A when the uplink interface of Switch A fails.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 120                 Running Pri  : 120
     Preempt Mode   : Yes                 Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : 10.1.1.4
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : 10.1.1.3
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 0
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1          State : Negative   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 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
    Auth Type      : None
    Virtual IP     : 10.1.1.1
    Member IP List : 10.1.1.4 (Local, Backup)
                     10.1.1.2 (Master)
                     10.1.1.3 (Backup)
  Forwarder Information: 3 Forwarders 2 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Active
    Virtual MAC    : 000f-e2ff-0011 (Take Over)
    Owner ID       : 0000-5e01-1101
    Priority       : 85
    Active         : local
    Redirect Time  : 93 secs
    Time-out Time  : 1293 secs
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 85
    Active         : 10.1.1.3
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that the weight of the VFs on Switch A decreases to 5 when Switch A fails. The state of all VFs on Switch A changes to Initialized, and cannot forward packets. Switch C becomes the AVF with virtual MAC address 000f-e2ff-0011 mapped to it and forwards packets sent by the hosts.

Display detailed information about VRRP group 1 on Switch C when the timeout timer timed out.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 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
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
```

```
                  10.1.1.3 (Backup)
  Forwarder Information: 2 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : 10.1.1.3
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that when the timeout timer timed out, the VF mapped to virtual MAC address 000f-e2ff-0011 is removed.

Display detailed information about VRRP group 1 on Switch B when Switch A fails.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     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      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.3 (Local, Master)
                      10.1.1.4 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
```

```
  Priority       : 127
  Active         : 10.1.1.4
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that Switch B has a higher priority than Switch C, and it will become the master after Switch A fails.

Configuration files

- Switch A:

```
#
 vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ip address 20.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface3
#
```

- Switch B:

```
#
 vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 30.1.1.2 255.255.255.0
```

```
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface3
#
```

- Switch C:

```
#
 vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.4 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 40.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface3
#
```

IPv6-based VRRP configuration examples

This chapter provides IPv6-based VRRP configuration examples.

Example: Configuring a single VRRP group

Applicable product matrix

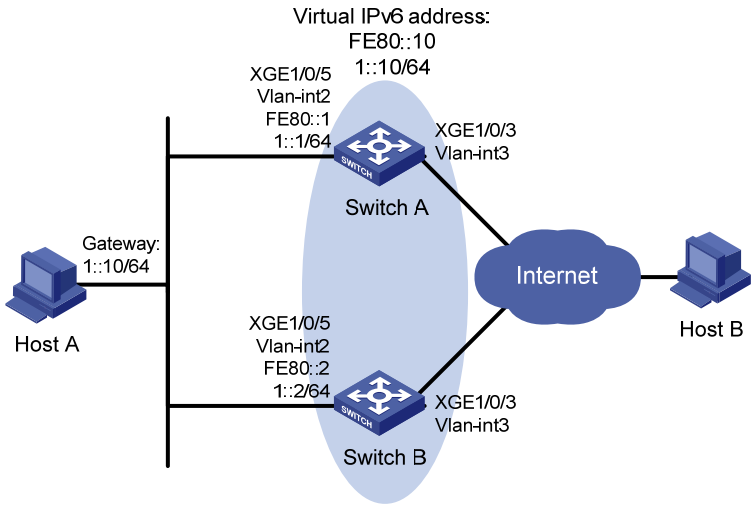
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 260, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet 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.

Figure 260 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.

Configuration procedures

1. Configure Switch A:

Configure VLAN 3.

```
<SwitchA> system-view
[SwitchA] vlan 3
[SwitchA-vlan3] port ten-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 ten-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 Switch A 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.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5
```

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:

Configure VLAN 3.

```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-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 ten-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 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 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 Virtual Router Information:
 Running Mode      : Standard
 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      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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
     Auth Type      : None
     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.

When Switch A fails, verify that Host A can still ping Host B. (Details not shown.)

Display detailed information about VRRP group 1 on Switch B.

```
IPv6 Virtual Router Information:
 Running Mode      : Standard
```

```
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      : None
    Virtual IP     : FE80::10
                     1::10
    Virtual MAC    : 0000-5e00-0201
    Master IP      : FE80::2
```

The output shows that when Switch A fails, Switch B becomes the master to forward packets from Host A to Host B.

Configuration files

- Switch A:

```
#
 vlan 2 to 3
#
interface Vlan-interface2
 ipv6 address FE80::1 link-local
 ipv6 address 1::1/64
 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 priority 110
 vrrp ipv6 vrid 1 preempt-mode delay 5
#
interface Vlan-interface3
 ipv6 address 2003::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

- Switch B:

```
#
 vlan 2 to 3
#
interface Vlan-interface2
 ipv6 address FE80::2 link-local
 ipv6 address 1::2/64
 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 delay 5
#
interface Vlan-interface3
 ipv6 address 2004::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring a track entry to monitor the uplink on the master by using interface management

Applicable product matrix

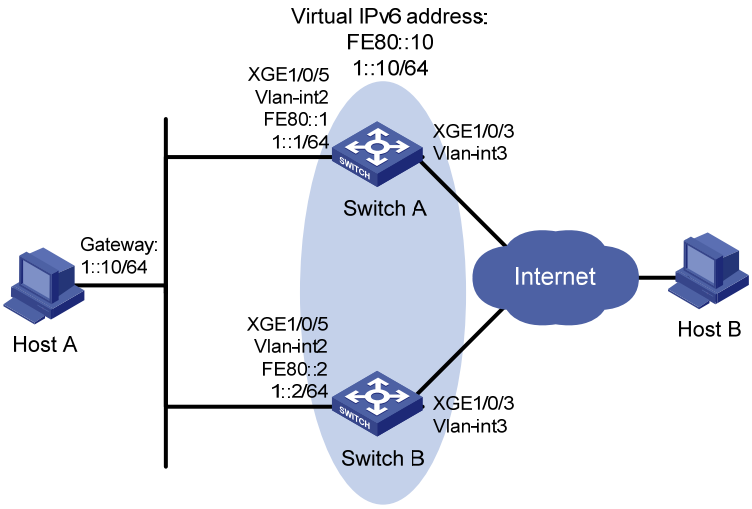
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 261, configure a VRRP group on Switch A and Switch B as the gateway for the hosts to meet the following requirements:

- Switch A operates as the master. When Switch A or its uplink interface fails, Switch B takes over to forward packets for the hosts.
- Create a track entry to monitor the uplink state on Switch A by using the interface management module. When the uplink fails, the priority of Switch A decreases, and Switch B takes over quickly to forward traffic.

Figure 261 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.

Configuration procedures

1. Configure Switch A:

   # Configure track entry 1 to monitor the link status of the uplink interface VLAN-interface 3 by using the interface management module.

   ```
   <SwitchA> system-view
   [SwitchA] track 1 interface vlan-interface 3
   ```

   # Configure VLAN 3 and the IPv6 address for VLAN-interface 3.

   ```
   [SwitchA] vlan 3
   [SwitchA-vlan3] port ten-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 and the IPv6 address for VLAN-interface 2.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] port ten-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 on VLAN-interface 2, and set its virtual IPv6 address 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
   ```

Set the priority of Switch A in VRRP group 1 to 110.

```
[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 delay 5
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 30 when the state of track entry 1 changes to negative.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 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:

Configure VLAN 3 and the IPv6 address for VLAN-interface 3.

```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-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 and the IPv6 address for VLAN-interface 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port ten-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 on VLAN-interface 2, and set its virtual IPv6 address 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 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 Host A:

Configure the default gateway of Host A as 1::10/64. (Details not shown.)

Verifying the configuration

Ping Host B from Host A to verify that the two hosts are reachable to each other. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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      : None
    Virtual IP     : FE80::10
                     1::10
    Virtual MAC    : 0000-5e00-0201
    Master IP      : FE80::1
  VRRP Track Information:
    Track Object   : 1                  State : Up         Pri Reduced : 30
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
```

The output shows that in VRRP group 1, Switch A is the master, and Switch B is a backup. Packets from Host A to Host B are forwarded through Switch A.

When Switch A fails, verify that Host A can still ping Host B. (Details not shown.)

Display detailed information about VRRP group 1 on Switch B.

```
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::2
```

The output shows that when Switch A fails, Switch B becomes the master. Packets from Host A to Host B are forwarded through Switch B.

When VLAN-interface 3 on Switch A fails, 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 ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::2
   VRRP Track Information:
     Track Object   : 1                  State : Up         Pri Reduced : 30
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
Running Mode      : Standard
 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      : None
     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 fails, the priority of Switch A decreases to 80. Switch A becomes the backup, and Switch B becomes the master. Packets from Host A to Host B are forwarded through Switch B.

Configuration files

- Switch A:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ipv6 address FE80::1 link-local
 ipv6 address 1::1/64
 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 priority 110
 vrrp ipv6 vrid 1 preempt-mode delay 5
```

```
 vrrp ipv6 vrid 1 track 1 reduced 30
#
interface Vlan-interface3
 ipv6 address 2003::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
 track 1 interface Vlan-interface3
#
```

- Switch B:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ipv6 address FE80::2 link-local
 ipv6 address 1::2/64
 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 delay 5
#
interface Vlan-interface3
 ipv6 address 2004::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
```

Example: Configuring multiple VRRPv3 groups for load balancing

Applicable product matrix

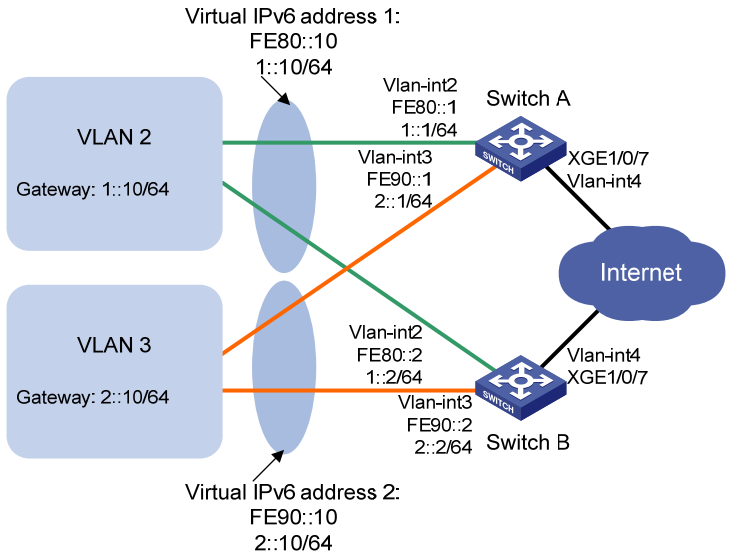
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 262, configure two VRRP groups on Switch A and Switch B to meet the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from Area A. 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.
- Create a track entry to monitor the uplink state on the switches by using the interface management module. When the uplink fails, the priority of the corresponding switch decreases, and the other switch takes over quickly to forward traffic.

Figure 262 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.

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 them is also the same.
- When you configure the value by which the priority of a switch decreases, make sure the decreased priority of the switch is lower than the priority of all the other switches in the VRRP group. This makes ensure a switch in the group can be elected as the master.

Configuration procedures

1. Configure Switch A:

   # Configure VLAN 4.

```
<SwitchA> system-view
[SwitchA] vlan 4
[SwitchA-vlan4] port ten-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 track entry 1 to monitor the link status of the uplink interface VLAN-interface 4 by using the interface management module.

```
[SwitchA] track 1 interface vlan-interface 4
```

   # Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port ten-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 delay 5
```

   # Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 30 when the state of track entry 1 changes to negative.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 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 ten-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 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:

Configure VLAN 4.

```
<SwitchB> system-view
[SwitchB] vlan 4
[SwitchB-vlan4] port ten-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 track entry 1 to monitor the link status of the uplink interface VLAN-interface 4 by using the interface management module.

```
[SwitchB] track 1 interface vlan-interface 4
```

Configure VLAN 2.

```
[SwitchB-vlan2] port ten-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 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 ten-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 delay 5
```

Associate VRRP group 2 on VLAN-interface 3 with track entry 1. Decrease the priority of the switch in the VRRP group by 30 when the state of track entry 1 changes to negative.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 track 1 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.

```
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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 Object   : 1                  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
     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 Virtual Router Information:
 Running Mode      : Standard
 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
```

```
  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 Object   : 1             State : Up             Pri Reduced : 30
```

The output shows that 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 Virtual Router Information:
 Running Mode      : Standard
 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 Object   : 1             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.

When VLAN-interface 4 on Switch A fails, hosts in VLAN 2 can still access the external network.

Display detailed information about the VRRP groups on Switch A.

```
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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 Object    : 1              State : Up              Pri Reduced : 30
```

Display detailed information about the VRRP groups on Switch B.

```
IPv6 Virtual Router Information:
 Running Mode      : Standard
 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      : 202.38.160.100
     Virtual MAC     : 0000-5e00-011e
     Master IP       : 202.38.160.2

   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     : 202.38.160.200
  Virtual MAC    : 0000-5e00-0120
  Master IP      : 202.38.160.131
VRRP Track Information:
  Track Object   : 1                  State : Up         Pri Reduced : 30
```

The output shows that when VLAN-interface 4 on Switch A fails, the priority of Switch A decreases to 80. Switch A becomes the backup, and Switch B becomes the master in VRRP group 1. Internet traffic for hosts in VLAN 2 is forwarded through Switch B.

Configuration files

- Switch A:

```
#
 vlan 2 to 4
#
interface Vlan-interface2
 ipv6 address 1::1 64
 ipv6 address FE80::1 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 priority 110
 vrrp ipv6 vrid 1 preempt-mode delay 5
 vrrp ipv6 vrid 1 track 1 reduced 30
#
interface Vlan-interface3
 ipv6 address 2::1 64
 ipv6 address FE90::1 link-local
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 2 virtual-ip FE90::10 link-local
 vrrp ipv6 vrid 2 virtual-ip 2::10
 vrrp ipv6 vrid 2 preempt-mode delay 5
#
interface Vlan-interface4
 ipv6 address 2000::2/64
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/6
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/7
 port access vlan 4
#
 track 1 interface Vlan-interface4
```

```
#
```

- Switch B:

```
#
 ipv6
#
 vlan 2 to 4
#
interface Vlan-interface2
 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 delay 5
#
interface Vlan-interface3
 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 delay 5
 vrrp ipv6 vrid 2 track 1 reduced 30
#
interface Vlan-interface4
 ipv6 address 2001::2/64
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/6
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/7
 port access vlan 4
#
 track 1 interface Vlan-interface4
#
```

Example: Using VRRPv3 with MSTP

Applicable product matrix

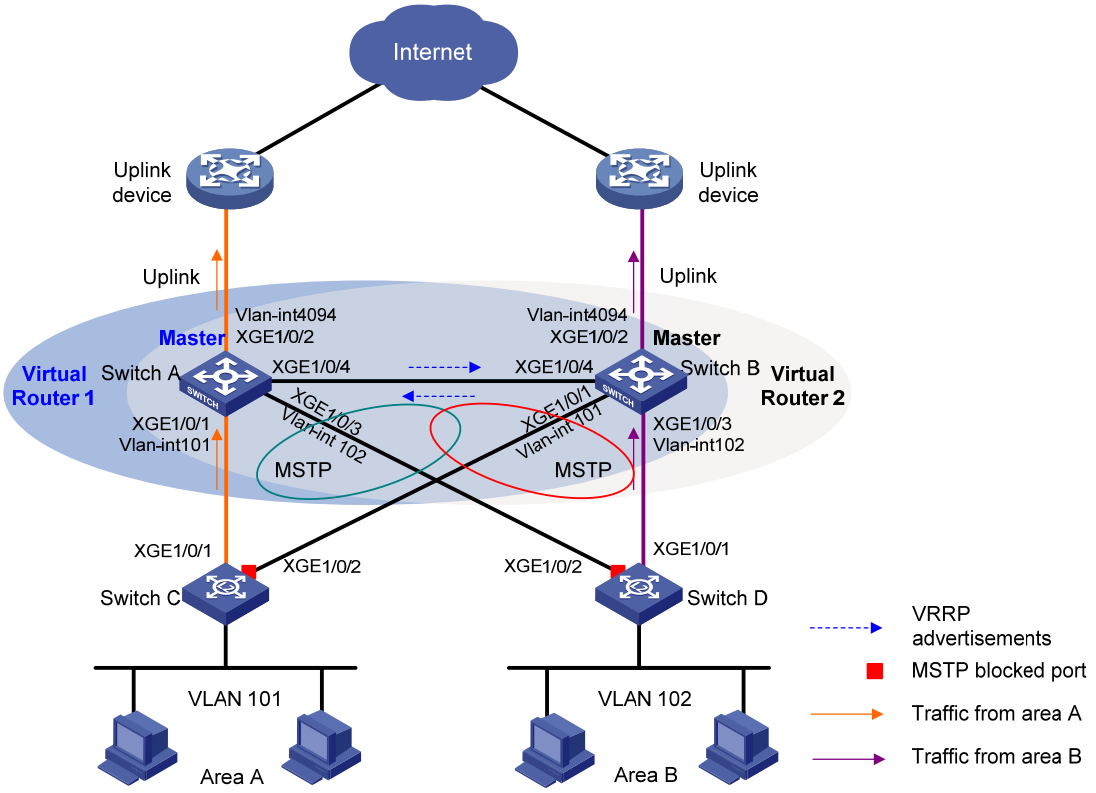
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 263, configure two VRRP groups on Switch A and Switch B to meet the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2. 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.
- Create a track entry to monitor the uplink state on the switches by using the interface management module. When the uplink fails, the priority of the corresponding switch decreases, and the other switch takes over quickly to forward traffic.

Figure 263 Network diagram



Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid loops between Switch A, Switch B, Switch C, and Switch D, enable MSTP on them.

Configuration procedures

1. Configure Switch A:

   # Assign Ten-GigabitEthernet 1/0/1 to VLAN 101, Ten-GigabitEthernet 1/0/3 to VLAN 102, and Ten-GigabitEthernet 1/0/2 to VLAN 4092.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] port ten-gigabitethernet 1/0/1
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port ten-gigabitethernet 1/0/3
[SwitchA-vlan102] quit
[SwitchA] vlan 4092
[SwitchA-vlan4092] port ten-gigabitethernet 1/0/2
[SwitchA-vlan4092] quit
```

   # Configure the link type of Ten-GigabitEthernet 1/0/4 as trunk.

```
[SwitchA] interface ten-gigabitethernet 1/0/4
[SwitchA-Ten-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/4] undo port trunk permit vlan 1
```

   # Assign Ten-GigabitEthernet 1/0/4 to VLAN 101 and VLAN 102.

```
[SwitchA-Ten-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchA-Ten-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchA-Ten-GigabitEthernet1/0/4] quit
```

   # Configure the uplink interface.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] undo stp enable
[SwitchA-Ten-GigabitEthernet1/0/2] quit
[SwitchA] interface vlan-interface 4092
[SwitchA-Vlan-interface4092] ipv6 address 2003::2 64
[SwitchA-Vlan-interface4092] quit
```

   # Configure track entry 1 to monitor the link status of the uplink interface VLAN-interface 4092 by using the interface management module.

```
[SwitchA] track 1 interface vlan-interface 4092
```

   # 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
```

On VLAN-interface 101, set the interface to be tracked to VLAN-interface 4092. The priority of VRRP group 1 on VLAN-interface 4092 will decrement by 20 when VLAN-interface 101 is down or removed.

```
[SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 track 1 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 global enable
```

2. Configure Switch B:

Assign Ten-GigabitEthernet 1/0/1 to VLAN 101, Ten-GigabitEthernet 1/0/3 to VLAN 102, and Ten-GigabitEthernet 1/0/2 to VLAN 4093.

```
<SwitchB> system-view
[SwitchB] vlan 101
[SwitchB-vlan101] port ten-gigabitethernet 1/0/1
[SwitchB-vlan101] quit
[SwitchB] vlan 102
[SwitchB-vlan102] port ten-gigabitethernet 1/0/3
[SwitchB-vlan102] quit
[SwitchB] vlan 4093
[SwitchB-vlan4093] port ten-gigabitethernet 1/0/2
[SwitchB-vlan4093] quit
```

Configure the link type of Ten-GigabitEthernet 1/0/4 as trunk.

```
[SwitchB] interface ten-gigabitethernet 1/0/4
[SwitchB-Ten-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/4] undo port trunk permit vlan 1
```

Assign Ten-GigabitEthernet 1/0/4 to VLAN 101 and VLAN 102.

```
[SwitchB-Ten-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchB-Ten-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchB-Ten-GigabitEthernet1/0/4] quit
```

Configure the uplink interface.

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] undo stp enable
[SwitchB-Ten-GigabitEthernet1/0/2] quit
[SwitchB] interface vlan-interface 4093
[SwitchB-Vlan-interface4093] ipv6 address 2004::2 64
[SwitchB-Vlan-interface4093] quit
```

Configure track entry 1 to monitor the link status of the uplink interface VLAN-interface 4093 by using the interface management module.

```
[SwitchB] track 1 interface vlan-interface 4093
```

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
```

On VLAN-interface 102, set the interface to be tracked to VLAN-interface 4093. The priority of VRRP group 1 on VLAN-interface 4093 will decrement by 20 when VLAN-interface 102 fails.

```
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 track 1 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 global enable
```

3. Configure Switch C:

Configure VLAN 101.

```
<SwitchC> system-view
[SwitchC] vlan 101
[SwitchC-vlan101] port ten-gigabitethernet 1/0/1 to ten-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 global enable
```

4. Configure Switch D:

   # Configure VLAN 102.

```
<SwitchD> system-view
[SwitchD] vlan 102
[SwitchD-vlan102] port ten-gigabitethernet 1/0/1 to ten-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 global 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. Execute the **display stp brief** command to display brief information about MSTP. (Details not shown.)

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 global 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 1 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 Ten-GigabitEthernet1/0/1
 port access vlan 101
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 4092
 undo stp enable
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 102
#
interface Ten-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
#
 track 1 interface Vlan-interface4092
#
```

- 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 global 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 1 reduced 20
#
interface Vlan-interface4093
 ipv6 address 2004::2/64
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 101
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 4093
 undo stp enable
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 102
#
interface Ten-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
#
 track 1 interface Vlan-interface4093
#
```

- Switch C:

```
#
 vlan 101
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp global enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 101
#
interface Ten-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 global enable
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 102
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 102
#
```

Example: Configuring VRRPv3 load balancing mode

Applicable product matrix

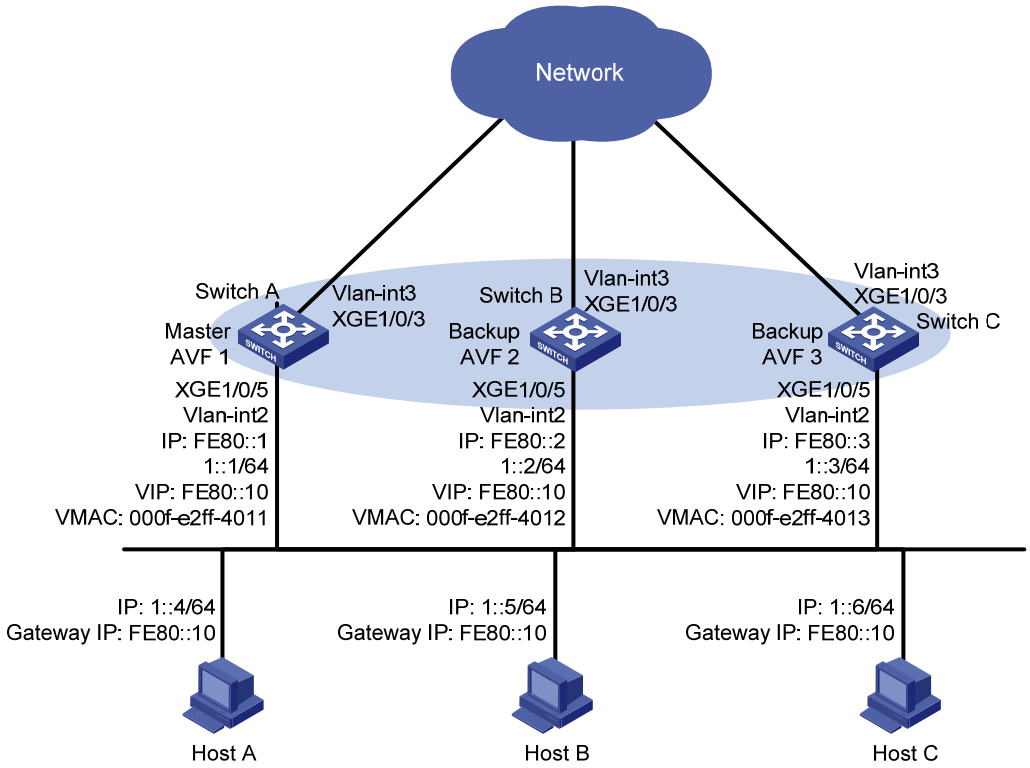
Product series	Software version
HP 5900	Release 2208P01
HP 5920	Release 2210

Network requirements

As shown in Figure 264, configure a load-balanced VRRP group on Switch A, Switch B, and Switch C to meet the following requirements:

- Switch A operates as the master to forward packets from Host A. When Switch A fails, Switch B or Switch C takes over to forward packets for Host A.
- Packets from the hosts are forwarded by different switches to reduce the burden of the master.
- Create a track entry to monitor the upstream link of the active virtual forwarder (AVF) by using the interface management module. When the upstream link of the AVF fails, the AVF can notify a listening virtual forwarder (LVF) to take over.

Figure 264 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.

Configuration restrictions and guidelines

When you configure VRRPv3 load balancing, follow these restrictions and guidelines:

- In load balancing mode, the virtual IPv6 address of a VRRP group can be any unassigned IPv6 address of the subnet where the VRRP group resides, rather than the IPv6 address of any interface in the VRRP group. No IP address owner can exist in a VRRP group.

- When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255 and does not change with the weight. To guarantee that an LVF can take over the VF owner as the AVF when the upstream link of the VF owner fails, the reduced weight for the VF owner must be higher than 245. This allows the weight of the VF owner to drop below the lower limit of failure.
- 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 Switch A:

   # Configure VLAN 3.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 3
   [SwitchA-vlan3] port ten-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 ten-gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   ```

   # Configure VRRP to operate in load balancing mode.

   ```
   [SwitchA] vrrp mode load-balance
   ```

   # Create VRRP group 1, and set the virtual IP address for the group to **FE80::10** and **1::10**.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
   ```

   # Set the priority of Switch A in VRRP group 1 to **120**.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 120
   ```

   # 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 delay 5
   ```

   # Enable Switch A to send RA messages, so the hosts in the subnet 1::/64 can learn the default gateway address.

   ```
   [SwitchA-Vlan-interface2] undo ipv6 nd ra halt
   [SwitchA-Vlan-interface2] quit
   ```

   # Create track entry 1 to monitor the link state of VLAN-interface 3 by using the interface management module.

   ```
   [SwitchA] track 1 interface vlan-interface 3
   ```

   # Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 250 when the state of track entry 1 changes to negative.

   ```
   [SwitchA] interface vlan-interface 2
   ```

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```

2. Configure Switch B:

   # Configure VLAN 3.

```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-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> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port ten-gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

   # Configure VRRP to operate in load balancing mode.

```
[SwitchB] vrrp mode load-balance
```

   # Create VRRP group 1, and set the virtual IP address for the group to **FE80::10** and **1::10**.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

   # Set the priority of Switch B in VRRP group 1 to **110**.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

   # 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 delay 5
```

   # Enable Switch B to send RA messages, so the hosts in the subnet 1::/64 can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit
```

   # Create track entry 1 to monitor the link state of VLAN-interface 3 by using the interface management module.

```
[SwitchB] track 1 interface vlan-interface 3
```

   # Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 250 when the state of track entry 1 changes to negative.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```

3. Configure Switch C:

   # Configure VLAN 3.

```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port ten-gigabitethernet 1/0/3
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ipv6 address 2005::2 64
```

```
[SwitchC-Vlan-interface3] quit
```

Configure VLAN 2.

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port ten-gigabitethernet 1/0/5
[SwitchC-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchC] vrrp mode load-balance
```

Create VRRP group 1, and set the virtual IP address for the group to **FE80::10** and **1::10**.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ipv6 address fe80::3 link-local
[SwitchC-Vlan-interface2] ipv6 address 1::3 64
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Configure Switch C to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5
```

Enable Switch C to send RA messages, so the hosts in the subnet 1::/64 can learn the default gateway address.

```
[SwitchC-Vlan-interface2] undo ipv6 nd ra halt
[SwitchC-Vlan-interface2] quit
```

Create track entry 1 to monitor the link state of VLAN-interface 3 by using the interface management module.

```
[SwitchC] track 1 interface vlan-interface 3
```

Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the switch in the VRRP group by 250 when the state of track entry 1 changes to negative.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```

Verifying the configuration

Ping the external network from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 120                Running Pri   : 120
     Preempt Mode   : Yes                Delay Time    : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
```

```
                    FE80::3 (Backup)
  Forwarder Information: 3 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Active
    Virtual MAC    : 000f-e2ff-4011 (Owner)
    Owner ID       : 0000-5e01-1101
    Priority       : 255
    Active         : local
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-4012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : FE80::2
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-4013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : FE80::3
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 110                 Running Pri  : 110
     Preempt Mode   : Yes                 Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::2 (Local, Backup)
                      FE80::1 (Master)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-4011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
```

```
    Active          : FE80::1
   Forwarder 02
    State           : Active
    Virtual MAC     : 000f-e2ff-4012 (Owner)
    Owner ID        : 0000-5e01-1103
    Priority        : 255
    Active          : local
   Forwarder 03
    State           : Listening
    Virtual MAC     : 000f-e2ff-4013 (Learnt)
    Owner ID        : 0000-5e01-1105
    Priority        : 127
    Active          : FE80::3
  Forwarder Weight Track Information:
    Track Object    : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 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
     Auth Type       : None
     Virtual IP      : FE80::10
                       1::10
     Member IP List  : FE80::3 (Local, Backup)
                       FE80::1 (Master)
                       FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight   : 255
     Running Weight  : 255
    Forwarder 01
     State           : Listening
     Virtual MAC     : 000f-e2ff-4011 (Learnt)
     Owner ID        : 0000-5e01-1101
     Priority        : 127
     Active          : FE80::1
    Forwarder 02
     State           : Listening
     Virtual MAC     : 000f-e2ff-4012 (Learnt)
     Owner ID        : 0000-5e01-1103
     Priority        : 127
     Active          : FE80::2
    Forwarder 03
     State           : Active
```

```
    Virtual MAC    : 000f-e2ff-4013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that in VRRP group 1, Switch A is the master, and Switch B and Switch C are the backups. An active VF and two listening VFs exist on each switch.

Display detailed information about VRRP group 1 on Switch A when the uplink interface of Switch A fails.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : FE80::3
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : FE80::2
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 0
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1          State : Negative   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 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
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-4011 (Take Over)
     Owner ID       : 0000-5e01-1101
     Priority       : 85
     Active         : local
     Redirect Time  : 93 secs
     Time-out Time  : 1293 secs
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 85
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that the weight of the VFs on Switch A decreases to 5 when Switch A fails. The state of all VFs on Switch A changes to Initialized, and cannot forward packets. Switch C becomes the AVF with virtual MAC address 000f-e2ff-0011 mapped to it and forwards packets sent by the hosts.

Display detailed information about VRRP group 1 on Switch C when the timeout timer timed out.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
```

```
 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
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that when the timeout timer timed out, the VF mapped to virtual MAC address 000f-e2ff-0011 is removed.

Display detailed information about VRRP group 1 on Switch B when Switch A fails.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 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      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::2 (Local, Master)
                      FE80::3 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
```

```
 Running Weight : 255
Forwarder 02
 State          : Active
 Virtual MAC    : 000f-e2ff-4012 (Owner)
 Owner ID       : 0000-5e01-1103
 Priority       : 255
 Active         : local
Forwarder 03
 State          : Listening
 Virtual MAC    : 000f-e2ff-4013 (Learnt)
 Owner ID       : 0000-5e01-1105
 Priority       : 127
 Active         : FE80::3
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that Switch B has a higher priority than Switch C, and it will become the master after Switch A fails.

Configuration files

- Switch A:

```
#
vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ipv6 address 1::1 64
 ipv6 address FE80::1 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 priority 120
 vrrp ipv6 vrid 1 preempt-mode delay 5
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 2003::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface3
#
```

- Switch B:

```
#
vrrp mode load-balance
#
vlan 2 to 3
#
interface Vlan-interface2
 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 priority 110
 vrrp ipv6 vrid 1 preempt-mode delay 5
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 2004::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface3
#
```

- Switch C:

```
#
vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ipv6 address 1::3 64
 ipv6 address FE80::3 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 delay 5
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 2005::2/64
#
interface Ten-GigabitEthernet1/0/3
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/5
```

```
 port access vlan 2
#
track 1 interface vlan-interface3
#
```